

490

P88

811.161.1:004(=512.133)  
004/038)

УЗБЕКСКОЕ АГЕНТСТВО СВЯЗИ И ИНФОРМАТИЗАЦИИ  
ЦЕНТР НАУЧНО-ТЕХНИЧЕСКИХ И МАРКЕТИНГОВЫХ  
ИССЛЕДОВАНИЙ

**РУССКО-УЗБЕКСКИЙ ТОЛКОВЫЙ СЛОВАРЬ  
ТЕРМИНОВ ПО ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ**

---

ЎЗБЕКИСТОН АЛОҚА ВА АХБОРОТЛАШТИРИШ АГЕНТЛИГИ  
ФАН-ТЕХНИКА ВА МАРКЕТИНГ ТАДҚИҚОТЛАРИ МАРКАЗИ

**АХБОРОТ ХАВФСИЗЛИГИГА ОИД ТЕРМИНЛАРНИНГ  
РУСЧА-ЎЗБЕКЧА ИЗОҲЛИ ЛУҒАТИ**

17. 12. 2009

Тошкент  
Ўзбекистон Республикаси Фанлар академияси  
«Фан» нашриёти  
2009

Под общей редакцией зам. директора Центра научно-технических  
и маркетинговых исследований З. Гиясова

Составитель: С. Абрамова

Перевод и редакция Ё. Ахмедовой, Ш. Тулаганова

Компьютерный набор: Б.Шамшиева

Эксперт О. Ахмедова

---

Фан-техника ва маркетинг тадқиқотлари маркази директорининг  
ўринбосари З. Гиясовнинг умумий таҳрири остида

Луғат С. Абрамова томонидан тузилди

Ё. Ахмедова, Ш. Тулагановлар томонидан таржима ва таҳрир  
килинди

Компьютер ишлари: Б. Шамшиева

Эксперт О.Ахмедова

ISBN 978-9943-09-870-1

© Ўзбекистон Республикаси ФА  
«Фан» нашриёти, 2009 йил.

## Введение

Характерной чертой последних десятилетий прошлого века стало беспрецедентное по темпам развитие современных информационно-коммуникационных технологий (ИКТ), включающих новые средства телекоммуникаций, обработки информации и коммуникации. Уровень развития информатизации общества решающим образом влияет на экономику, обороноспособность и политику и является одной из важных геополитических задач каждого государства.

Революционное воздействие ИКТ касается взаимодействия государственных структур и институтов гражданского общества, экономической и социальной сфер, науки и образования, культуры и образа жизни людей. Многие развитые и развивающиеся страны в полной мере осознали те колоссальные преимущества, которые несет с собой развитие и распространение информационно-коммуникационных технологий.

Но и у информационной революции, как и у всякого явления, есть оборотная сторона медали. Всеобщая компьютеризация основных сфер деятельности и стремительное развитие сети Интернет ведет к появлению широкого спектра внутренних и внешних угроз: нетрадиционных каналов утечки информации и каналов несанкционированного доступа к ней.

В современных условиях проблема защиты информации от несанкционированного доступа, распространения недостоверной информации, нарушения нормального функционирования информационных систем из-за внедрения в них «компьютерных вирусов» становится особенно остро.

Терминология играет значительную роль во всех областях жизнедеятельности общества, и сфера информационной безопасности не является исключением. Русско-узбекский толковый словарь терминов по информационной безопасности является попыткой обобщить имеющуюся терминологию в сфере информационной безопасности и, безусловно, не является исчерпывающим. Словарь – результат работы специалистов Службы терминологии и словарей, а также Центра научно-технических и маркетинговых исследований. Он включает в себя около 1400 терминов, расположенных в алфавитном порядке. В нем отражены термины и определения на русском и узбекском языках и эквиваленты этих терминов на английском языке.

Словарь может быть полезен специалистам в сфере информатизации, руководителям хозяйствующих субъектов при выработке политики информационной безопасности, студентам и аспирантам соответствующих специальностей, а также широкому кругу людей, интересующихся проблемами обеспечения информационной безопасности.

Заранее выражаем признательность за замечания и предложения. Они будут учтены при подготовке очередного издания словаря.

## Кириш

Телекоммуникациялар, ахборотни қайта ишлаш ва коммуникацияларнинг янги воситаларини ичига олувчи замонавий ахборот-коммуникация технологиялари (АКТ) нинг мислсиз ривожланиш суръатлари ўтган аср сўнгги ўн йилликларининг ўзига хос хусусияти бўлди. Жамиятни ахборотлаштиришни ривожлантириш даражаси иқтисодиётга, мудофаа қобилиятига, сиёсатга катта таъсир кўрсатади ва ҳар бир давлатнинг муҳим геосиёсий вазибаларидан бири ҳисобланади.

Ахборот-коммуникация технологияларининг тубдан ўзгартирувчи таъсири давлат структуралари ва фуқаролик жамияти институтларининг ўзаро ҳамкорлигига, иқтисодий ва ижтимоий соҳаларига, фан ва таълим, одамларнинг турмуш тарзи ҳамда маданиятига дахлдир. Ривожланган ва ривожланаётган кўплаб мамлакатларда ахборот-коммуникация технологияларининг ривожланиши ва жорий қилиниши вужудга келтирадиган афзалликлар тўла англаб етилган.

Бироқ ҳар бир воқеа-ҳодисада бўлгани каби, ахборот технологияларининг ривожланиши, жорий қилиниши борасида ҳам ўзига хос мураккабликлар мавжуд. Жумладан, фаолиятнинг асосий соҳаларини ялпи компьютерлаштириш ва Интернет тармоғининг жадал ривожланиши кўплаб ташқи ва ички таҳдидлар, масалан, ахборот чиқиб кетиши мумкин бўлган ноанъанавий каналлар ҳамда ахборотдан руҳсат этилмаган тарзда фойдалана олиш каналлари пайдо бўлишига олиб келади.

Ҳозирги шароитларда ахборотни руҳсат этилмаган тарзда фойдалана олишдан муҳофаза қилиш, ишончли бўлмаган ахборотнинг тарқалиб кетиши, «компьютер вирусларининг» киритилиши оқибатида ахборот тизимлари нормал ишлашининг издан чиқиши муаммоси айниқса кескинлашади.

Атамашунослик жамият ҳаётининг барча соҳаларида, шу жумладан, ахборот хавфсизлиги соҳасида ҳам сезиларли рол ўйнайди. Ахборот хавфсизлигига оид атамаларнинг русча-ўзбекча изоҳли луғати ахборот хавфсизлиги соҳасидаги, бу соҳа билан боғлиқ атамаларни умумлаштиришга бўлган дастлабки уринишдир, бинобарин, луғатни мукамал деб бўлмайди. Луғат Атамашунослик ва луғатлар хизмати мутахассисларининг, шунингдек, Фан-техника ва маркетинг тадқиқотлари Маркази бошқа бир гуруҳ мутахассисларининг меҳнати самарасидир. Луғат алифбо тартибда жойлаштирилган 1400 га яқин атамани ўз ичига олади. Луғатда рус ва ўзбек тилларидаги атамалар ва таърифлар ҳамда шу атамаларнинг инглиз тилидаги муқобиллари келтирилган.

Луғатдан ахборотлаштириш соҳасида ишловчи мутахассислар, хўжалик юритувчи субъектларнинг раҳбарлари ахборот хавфсизлиги бўйича сиёсатни ишлаб чиқишда, тегишли ихтисосликдаги талабалар ва аспирантлар, шунингдек, ахборот хавфсизлигини таъминлаш муаммолари билан қизикувчиларнинг кенг оммаси фойдаланишлари мумкин.

Луғат юзасидан билдириладиган фикр-мулоҳазалар ва таклифлар учун олдиндан миннатдорчилик билдирамыз. Улар луғатнинг кейинги нашрини тайёрлашда ҳисобга олинади.

| Термин | Определение |
|--------|-------------|
|--------|-------------|

## А

**Аварийный**  
**uz** - авария(вий)  
**en** - emergency

Определение, характеризующее анализ причин возникновения нежелательных ситуаций в работе системы, основанный на информации, записанной в момент обнаружения нежелательной ситуации.

**Автоконтроль целостности**

**uz** - яхлитликни  
автоназорат қилиш  
**en** - integrity  
autocontrol

Использование в программе специальных алгоритмов, позволяющих после запуска программы определить, были ли внесены изменения в файл, из которого загружена программа, или нет.

Дастурда, дастур ишга туширилгандан сўнг, дастур юкланган файлга ўзгаришлар киритилган-киритилмаганлигини аниқлаш имконини берадиган махсус алгоритмлардан фойдаланиш.

**Автокорреляция**  
**uz** - автокорреляция  
**en** - autocorrelation

Мера подобия различных частей одного и того же множества данных; в контексте проблемы распознавания (идентификации) программ может служить мерой подлинности.

Айнан бир маълумотлар тўплами турли қисмларининг ўхшашлик ўлчови; дастурларни аниқлаш (идентификация қилиш) муаммоси контекстда ҳақиқийлик ўлчови бўлиб хизмат қилиши мумкин.

**Авторизация**  
**uz** - муаллифлаштириш

1. Предоставление прав, которое включает предоставление доступа на основании прав доступа.

## A

en - authorization

2. Проверка прав доступа пользователя и получением им доступа к ресурсам в соответствии с данными ему правами.
3. Предоставление субъекту прав на доступ к объекту.
4. Предоставление доступа пользователю, программе или процессу.
5. Предоставление доступа к различным системным ресурсам или отказ в доступе. Авторизации обычно предшествует процедура аутентификации.

1. Фойдаланиш ҳуқуқлари асосида фойдаланиш имкониятини тақдим этишдан иборат бўлган ҳуқуқларни тақдим этиш.
2. Фойдаланувчининг эркин фойдаланиш ҳуқуқларини текшириш ва унга берилган ҳуқуқларга мувофиқ ресурслардан фойдаланишга руҳсат олиш.
3. Субъектга объектга қира олиш ҳуқуқларини тақдим этиш.
4. Фойдаланувчи, дастур ёки жараёнга қира олишни тақдим этиш.
5. Турли хилдаги тизим ресурсларидан фойдаланишни тақдим этиш ёки фойдаланишнинг рад этилиши. Муаллифлаштириш одатда аутентификация процедурасидан илгари бўлади.

**Авторизация данных**

uz - маълумотларни муаллифлаштириш  
en - data authorization

Определение и установление степени приватности данных в базе данных.

Маълумотлар базасидаги маълумотларнинг хусусийлик даражасини аниқлаш ва белгилаш.

**Авторизация программы**

uz - дастурни муаллифлаштириш

Установление ограничения на доступ к системной или пользовательской программе со стороны других программ и пользователей.

## А

**en - program authorization**

Тизим ёки фойдаланувчи дастуридан бошқа дастурлар ёки фойдаланувчиларнинг фойдалана олиши бўйича чеклашларнинг ўрнатилиши.

### **Агрегирование**

**uz - агрегирлаш (бирлаштириш)**

**en - aggregation**

1. Получение чувствительной информации методом сбора и сопоставления информации меньшей чувствительности.
2. Способ получения конфиденциальной (защищаемой) информации на основе обобщения сведений меньшей степени конфиденциальности или открытой информации.

1. Таъсирчанлиги камрок бўлган ахборотни тўплаш ва қиёслаш методи ёрдамида таъсирчан ахборотни олиш.

2. Конфиденциаллик даражаси пастроқ бўлган маълумотларни умумлаштириш ёки очик ахборот асосида конфиденциал (муҳофаза қилинадиган) ахборотни олиш усули.

**Администратор базы данных**

**uz - маълумотлар базаси маъмури**

**en - database administrator**

Специальное должностное лицо (группа лиц), имеющее(ие) полное представление о базе данных и отвечающее за ее ведение, использование и развитие. Входит в состав администрации банка данных.

Маълумотлар базаси тўғрисида тўлиқ тасаввурга эга бўлган ва бу маълумотлар базасини юритиш, ундан фойдаланиш, уни ривожлантириш юзасидан жавобгар махсус мансабдор шахс (шахслар гуруҳи). Маълумотлар банки маъмурияти таркибига кирди.

**Администратор безопасности (защиты)**

1. Полномочный представитель (лицо или группа лиц), ответственный за обеспечение безопасности системы, за реали-

## A

**uz** - хавфсизлик  
(муҳофаза қилиш)  
маъмури  
**en** - security (safety)  
administrator

зацию 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 сети (системы) телекоммуникаций от несанкционированного доступа к информации.

3. Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

1. Тизим хавфсизлигини таъминлаш, ўрнатилган маъмурий муҳофаза чораларини амалга ошириш ва уларга риоя қилинишининг узлуксизлиги учун жавобгар, қўлланиладиган жисмоний ва техник муҳофаза воситалари ишлашининг ташкилий жиҳатдан мунтазам қўллаб-қувватланишини амалга оширувчи ваколатли вакил (шахс ёки шахслар гуруҳи).

2. Телекоммуникациялар тармоғи (тизимлари)нинг ахборотдан рухсат этилмаган тарзда фойдаланишдан муҳофаза қилиниши юзасидан жавобгар, фойдаланиш субъекти.

3. Автоматлаштирилган тизимнинг ахборотдан рухсат этилмаган тарзда фойдаланишдан муҳофаза қилиниши учун жавобгар бўлган фойдалана олиш субъекти.

**Администратор доступа**

**uz** - фойдалана олиш  
маъмури  
**en** - access  
administrator

Одно из должностных лиц в составе администрации банка данных, отвечающее за организацию доступа пользователей к базам данных.

Маълумотлар банки маъмурияти тарки-



## А

бидаги фойдаланувчиларнинг маълумотлар базасидан эркин фойдаланишларини ташкиллаштириш учун жавобгар бўлган мансабдор шахслардан бири.

**Администратор  
межсетевого экрана**

**uz** - тармоқлараро  
экран маъмури  
**en** - firewall  
administrator

Лицо, ответственное за сопровождение межсетевого экрана.

Тармоқлараро экраннинг кузатиб борилиши юзасидан жавобгар шахс.

**Администратор  
системный**

**uz** - тизим маъмури  
**en** - system  
administrator

Лицо, отвечающее за эксплуатацию системы и поддержание ее в работоспособном состоянии

Тизимнинг эксплуатация қилиниши ва ишчи ҳолатда сақлаб турилиши юзасидан жавобгар шахс.

**Администратор  
службы  
безопасности**

**uz** - хавфсизлик хизмати маъмури  
**en** - Security service  
administrator

Лицо (или группа лиц), имеющее не полное представление об одной или нескольких системах обеспечения безопасности и контролирующее их проектирование и использование.

Битта ёки бир нечта хавфсизликни таъминлаш тизими тўғрисида тўлиқ тасаввурга эга бўлган, уларнинг лойиҳалаштирилишини ва улардан фойдаланишни назорат қилувчи шахс (ёки шахслар гуруҳи).

**Администрация  
банка данных**

**uz** - маълумотлар  
банки маъмурияти  
**en** - databank  
administration

Группа лиц (подразделение), отвечающих за эксплуатацию банка данных: ведение баз данных, организацию коллективного доступа к ним пользователей и развитие системы.

Маълумотлар банкidan фойдаланиш: маълумотлар базасини олиб бориш, ун-

## А

дан жамоа бўлиб фойдаланишни ташкиллаштириш ва тизимни ривожлантириш юзасидан жавобгар бўлган шахслар гуруҳи (бўлинма).

### **Администрация системы защиты**

**uz** - муҳофаза тизими  
маъмурияти  
**en** - security system  
administration

Орган управления, устанавливающий политику безопасности и определяющий объекты и субъекты, к которым данная политика применяется.

Хавфсизлик сиёсатини белгилайдиган ҳамда бу сиёсат қўлланиладиган объект ва субъектларни аниқлайдиган бошқарув органи.

### **Администрирование базы данных**

**uz** - маълумотлар ба-  
засини бошқариш  
**en** - database  
administration

Выполнение функций определения, организации, управления и защиты данных в базе данных.

Маълумотлар базасида маълумотларни белгилаш, ташкиллаштириш, бошқариш ва муҳофаза қилиш функцияларининг бажарилиши.

### **Администрирование средств безопасно- сти**

**uz** - хавфсизлик  
воситаларини  
бошқариш  
**en** - security facilities  
administration

Процесс, включающий распространение информации, необходимой для работы сервисов безопасности, а также сбор и анализ информации об их функционировании. Например, распространение криптографических ключей, установка прав доступа, анализ журнала аудита и т.п.

Хавфсизлик сервисларининг ишлаши учун зарур бўлган ахборотнинг тарқатилишини, шунингдек, уларнинг ишлаши тўғрисидаги ахборотни тўплаш ва таҳлил қилишни ичига оладиган жараён. Масалан, криптографик калитларнинг тарқатилиши, фойдалана олиш ҳуқуқининг ўрнатилиши, аудит журналининг таҳлили ва ш.к.

## А

### Аккредитация

uz - аккредитлаш

en - accreditation

Официальное признание технической компетентности предприятия и независимости его от разработчиков, изготовителей (поставщиков) и заказчиков (потребителей) испытываемых средств защиты информации для организации и проведения испытаний в соответствии с требованиями стандартов и иных нормативных документов. Аккредитацию осуществляет специально уполномоченный орган.

Корхонанинг техник компетентлигини ҳамда унинг стандартлар ва бошқа норматив хужжатлар талабларига мувофиқ, синовларни ташкил қилиш ва ўтказиш учун синаладиган ахборотни муҳофаза қилиш воситаларини ишлаб чиқувчилар, тайёрловчилар (етказиб берувчилар), бюрutmачилар (истеъмолчилар)дан мустақиллигини расман тан олиш. Аккредитлаш махсус ваколатли орган томонидан амалга оширилади.

### Аккредитация в области защиты информации

uz - ахборотни муҳофаза қилиш соҳасида аккредитлаш

en - accreditation in the field of information security

Официальное признание полномочий осуществлять какую-либо деятельность в области сертификации защищенных изделий, технических средств и способов защиты информации.

Муҳофазаланган махсулотлар, ахборотни муҳофаза қилиш техник воситалари ва усулларини сертификатлаш соҳасида қандайдир фаолиятни амалга ошириш бўйича ваколатларнинг расман тан олиниши.

### Активы информационные

uz - ахборот активлари

en - information asset

Информация или средства обработки информации юридического лица.

Юридик шахснинг ахбороти ёки ахборотни қайта ишлаш воситалари.

## A

- Алгоритм**  
**uz** - алгоритм  
**en** - algorithm
- Алгоритм DES**  
**трёхкратный**  
**uz** - уч мартали DES  
алгоритми  
**en** - 3DES (Triple  
DES)
- Алгоритм дешифрования**  
**uz** - дешифрлаш алгоритми  
**en** - decryption  
algorithm
- Алгоритм Диффи-Хеллмана**  
**uz** - Диффи-Хеллман  
алгоритми  
**en** - Diffie-Hellman algorithm
- Алгоритм имитозащищающего кодирования информации**  
**uz** - ахборотни имитомухофазаловчи
- Упорядоченный конечный набор четко определенных правил для решения задач за конечное количество шагов.
- Масала(лар)ни чекланган кадамларда ечиш учун аниқ белгиланган коидаларнинг тартибланган чекли тўплами.
- Метод шифрования, в котором алгоритм DES используется три раза с тремя различными ключами.
- DES алгоритмидан уч марта учта турли калит билан фойдаланиладиган шифрлаш методи.
- Алгоритм, реализующий функцию дешифрования.
- Дешифрлаш функциясини амалга оширадиган алгоритм.
- Алгоритм открытого распределения ключей, так-же называемый экспоненциальным распределением ключей, основанный на использовании односторонней показательной функции.
- Калитларни очик тақсимлаш, шунингдек, калитларни экспоненциал тақсимлаш деб номланувчи бир томонлама кўрсаткичли функциядан фойдаланишга асосланган алгоритм.
- Алгоритм преобразования информации с целью контроля целостности.
- Яхлитликни назорат қилиш мақсадида ахборотни ўзгартириш алгоритми.

кодлаш алгоритми  
**en** - information encoding imitoprotecting algorithm

**Алгоритм криптографический**  
**uz** - криптографик алгоритм  
**en** - cryptographic algorithm

**Алгоритм криптографический асимметричный**  
**uz** - асимметрик криптографик алгоритм  
**en** - asymmetric cryptographic algorithm

**Алгоритм криптографический симметричный**  
**uz** - симметрик криптографик алгоритм  
**en** - symmetric cryptographic algorithm

**Алгоритм проверки цифровой подписи**

Математический алгоритм преобразования информации (данных) с целью предотвратить возможность её искажения и защитить от несанкционированного доступа.

Ахборот (маълумотлар)ни, унинг бузиб кўрсатилиши мумкинлигининг олдини олиш ва рухсат этилмаган тарзда фойдаланишдан муҳофаза қилиш мақсадида қайта ўзгартиришнинг математик алгоритми.

Алгоритм выполнения шифрования или соответствующего дешифрования, при котором для шифрования и дешифрования используются разные ключи.

Шифрлаш ва дешифрлаш учун турли калитлардан фойдаланиладиган, шифрлаш ёки тегишли дешифрлашни бажариш алгоритми.

Алгоритм выполнения шифрования или соответствующий алгоритм выполнения дешифрования, в котором для шифрования и дешифрования требуется один и тот же ключ.

Шифрлаш ва дешифрлаш учун айнан битта калитдан фойдаланиладиган, шифрлаш ёки тегишлича дешифрлашни бажариш алгоритми.

Алгоритм, в качестве исходных данных которого используются подписанное со-

## А

**uz** - рақамли имзони текшириш алгоритми  
**en** - digital signature checking algorithm

общение, ключ проверки и параметры схемы цифровой подписи, а результатом является заключение о правильности или ошибочности цифровой подписи.

**Алгоритм СМЕА**  
**uz** - СМЕА алгоритми  
**en** - Cellular Message Encryption Algorithm (СМЕА)

Дастлабки маълумотлари сифатида имзоланган хабар, текшириш калити ва рақамли имзо схемаси параметрларидан фойдаланиладиган алгоритм, рақамли имзонинг тўғрилиги ёки хатолиги тўғрисидаги хулоса натижа ҳисобланади.

**Алгоритм**  
**Сторнетта-Хабера**  
**uz** - Сторнетт-Хабера алгоритми  
**en** - Stornett Khaber algorithm

Алгоритм шифрования сообщений в сетях цифровой сотовой связи (USDC).

Рақамли сотали алоқа тармоқларида хабарларни шифрлаш алгоритми.

Алгоритм, обеспечивающий подпись документов по времени без возможности их подделки.

**Алгоритм формирования цифровой подписи**  
**uz** - рақамли имзони шакллантириш алгоритми  
**en** - digital signature formation algorithm

Хужжатларнинг вақт бўйича, уларни қалбакилаштириш имконияти бўлмайдиган тарзда, имзоланишини таъминловчи алгоритм.

Алгоритм, в качестве исходных данных которого используются сообщение, ключ подписи и параметры схемы цифровой подписи, а в результате формируется цифровая подпись.

Дастлабки маълумотлари сифатида хабар, имзо калити ва рақамли имзо схемаси параметрларидан фойдаланиладиган алгоритм, натижада рақамли имзо шаклланади.

**Алгоритм хэширования односторон-**

Алгоритм хэширования, который обладает свойством практической невозмож-

## А

**ний**

**uz** - бир томонлама хэшлаш алгоритми  
**en** - single sided hashing algorithm

**Алгоритм шифрования**

**uz** - шифрлаш алгоритми  
**en** - encryption algorithm

**Алгоритм шифрования данных**

**uz** - маълумотларни шифрлаш алгоритми  
**en** - data encryption algorithm

**Алгоритм Эль-Гамала**

**uz** - Ал-Жамол алгоритми  
**en** - Ale Namale algorithm

ности восстановления на основе значения хэш-кода исходных данных, из которых этот хэш-код был получен.

Хэш-код олинган дастлабки маълумотларнинг хэш-код қиймати асосида амалда тиклаб бўлмаслик хоссасига эга бўлган хэшлаш алгоритми.

Алгоритм, реализующий функцию шифрования.

Шифрлаш функциясини амалга оширадиган алгоритм.

Набор математических правил, определяющих содержание и последовательность операций, зависящих от ключевой переменной (ключ шифрования), по преобразованию исходной формы представления информации (открытый текст) к виду, обладающему секретом обратного преобразования (зашифрованный текст).

Дастлабки матнни шифрланган матнга ва/ёки аксинча, алмаштириш бўйича калитли ўзгарувчига (шифрлаш калитига) боғлиқ бўлган амаллар мазмуни ва кетма-кетлигини белгиловчи криптографик алгоритм.

Криптосистема, базирующаяся на задаче дискретного логарифмирования, которая может использоваться как для шифрования, так и для аутентификации (цифровой подписи) информации.

Ахборотни аутентификация қилиш (Ракамли имзо) ҳамда шифрлаш учун фой-

## А

даланиладиган дискрет логарифмлаш масаласи асосидаги криптотизим.

### Амортизация отказа

**uz** - ишламай қолишлар амортизацияси  
**en** - fail soft

Свойство вычислительной системы, состоящее в способности распознавать изменения окружающей среды и выполнять свои функции в условиях отказа или изъятия части оборудования.

Ҳисоблаш тизимининг, атроф-муҳит ўзгаришини аниқлаш ва ускуна носоз бўлган ёки унинг бир қисми олиб ташланган шароитда ўз функцияларини бажара олишида акс этувчи хусусияти.

### Анализ затрат (выгоды)

**uz** - харажатлар (фойда) ни таҳлил қилиш  
**en** - costbenefit analysis

Стадия в разработке или функционировании системы, на которой определяется стоимость обеспечения требуемого уровня защиты данных в информационной системе. Иногда под этой стоимостью подразумевают ущерб, который может быть нанесен в случае утери или компрометации данных, подлежащих защите.

Тизимни ишлаб чиқиш ёки ишлашидаги босқич бўлиб, бунда ахборот тизимидаги маълумотларнинг талаб этиладиган даражада муҳофаза қилинишини таъминлаш қиймати аниқланади. Баъзида бу қиймат остида муҳофаза қилиниши лозим бўлган маълумотларнинг йўқолиши ёки путур етказилиши (обрўсизлантирилиши) оқибатида етказилиши мумкин бўлган зарар тушунилади.

### Анализ защищенности

**uz** - муҳофаза қилинганликни

1. Процесс обнаружения уязвимостей ресурсов автоматизированной системы, а также выработка рекомендаций по их устранению.



таҳлил қилиш  
en - protection analysis

2. Проверка соответствия качественных и количественных показателей эффективности мероприятий по защите информации требованиям по безопасности информации.

1. Автоматлаштирилган тизим ресурсларининг заиф жойларини аниқлаш, шунингдек, уларни бартараф қилиш бўйича тавсиялар ишлаб чиқиш жараёни.

2. Ахборотни муҳофаза қилиш бўйича тадбирлар самарадорлиги сифат ва миқдор кўрсаткичларининг ахборот хавфсизлиги талабларига мос келишини текшириш.

**Анализ криптографический**

uz - криптографик  
таҳлил қилиш  
en - cryptoanalysis

1. Искусство и наука вскрытия шифра или объекта криптографии, любой другой формы.

2. Процесс получения исходного текста по шифрованному без знания ключа или процесс вычисления ключа по исходному и шифрованному тексту.

1. Шифрни ёки ҳар қандай бошқа шаклдаги криптография объектининг сирини очиш санъати ва илми.

2. Қалитни билмасдан туриб шифрланган матндан дастлабки матни олиш ёки дастлабки матн ва шифрланган матн бўйича қалитни ҳисоблаб чиқариш жараёни.

**Анализ прерывания**

uz - узилишни таҳлил қилиш  
en - interrupt analysis

Функция, выполняемая обработчиком прерываний по коду в старом слове состояния программы (PSW) и состоящая в определении причины прерывания и выборе соответствующей программы его обработки.

(PSW) дастур ҳолати эски сўзидаги код бўйича узилишларни қайта ишловчи томонидан бажариладиган ва узилиш сабабини

## А

аниқлаш ҳамда уни қайта ишлашнинг тегишли дастурини танлашдан иборат функция.

### **Анализ программы санкционированный**

**uz** - дастурни рухсат этилган тарзда таҳлил қилиш

**en** - authorized program analysis

Анализ, выполняемый для установления расхождения между техническими требованиями и реальными возможностями программы.

Техник талаблар билан дастурнинг ҳақиқий имкониятлари ўртасидаги фарқни белгилаш мақсадида бажариладиган таҳлил.

### **Анализ риска**

**uz** - риск (эҳтимоллий хавф) ни таҳлил қилиш

**en** - risk analysis

1. Систематическое выполнение процедур идентификации ресурсов системы обработки данных, угроз этим ресурсам и уязвимостей системы к этим угрозам.

2. Процесс определения угроз безопасности системы в целом и отдельным ее компонентам (не только техническим), определения характеристик угроз и потенциального ущерба, который может быть нанесен в случае их реализации, а также разработка мер по защите.

1. Маълумотларни қайта ишлаш тизими ресурсларини, бу ресурсларга таҳдидларни ва бу таҳдидларга нисбатан тизимнинг заифликларини идентификация қилиш процедураларининг мунтазам бажарилиши.

2. Умуман тизим хавфсизлигига ва унинг алоҳида (нафақат техник) компонентларига таҳдидларни, таҳдидлар характеристикасини ва улар амалга оширилганда етказилиши мумкин бўлган потенциал зарарни аниқлаш, шунингдек, муҳофаза чоратадбирларини ишлаб чиқиш жараёни.

## А

### Анализ риска полный

**uz** - риск (эхтимолий хавф)ни тўлиқ таҳлил қилиш

**en** - full risk analysis

Анализ рисков для информационных систем, предъявляющих повышенные требования в области информационной безопасности (более высокие, чем базовый уровень защищенности).

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

Ахборот хавфсизлиги соҳасида оширилган (муҳофаза қилинганликнинг базавий даражасига қараганда юқорироқ бўлган) талаблар қўядиган ахборот тизимлари учун риск (эхтимолий хавф)ларни таҳлил қилиш.

*Изоҳ: Риск (эхтимолий хавф)ларни тўлиқ таҳлил қилиш ресурсларнинг қимматлиги аниқланишини, таҳдидлар ва заифликлар баҳолашини, адекват қарши чоралар танланишини ва уларнинг самарадорлиги баҳолашини кўзда тутати.*

### Анализ трафика

**uz** - трафикни таҳлил қилиш

**en** - traffic analysis

Анализ информации, полученной при наблюдении за потоками трафика. Например, анализ наличия, отсутствия, объема, направления и частоты трафика.

Трафик оқимларини кузатиш пайтида олинган ахборот таҳлили. Масалан, трафик мавжудлиги, мавжуд эмаслиги, ҳажми, йўналиши ва частотасининг таҳлили.

### Анализ угроз

**uz** - таҳдидларни таҳлил қилиш

**en** - threat analysis

Исследование действий и событий, которые могут неблагоприятно воздействовать на систему обработки данных.

Маълумотларни қайта ишлаш тизимига салбий таъсир этиши мумкин бўлган ҳаракатлар ва ҳодисаларни тадқиқ этиш.

## А

### **Анализатор**

**uz** - анализатор

**en** - analyzer

В системах программирования – алгоритм, выполняющий анализ исходной программы.

Дастурлаш тизимларида – дастлабки дастурнинг таҳлил қилинишини амалга оширувчи алгоритм.

### **Анализатор аварийного состояния**

**uz** - авария ҳолати

анализатори

**en** - emergency (disaster situation) analyzer

Программа, предназначенная для анализа аварийного состояния вычислительной системы и выдачи информации на печать.

Ҳисоблаш тизимининг авария ҳолатини таҳлил қилиш ва ахборотни босишга бериш учун мўлжалланган дастур.

### **Анализатор прерываний**

**uz** - узилишлар ана-

лизатори

**en** - interrupt analyzer

Машинная программа, определяющая возможность возникновения конфликтов в системе в результате прерываний.

Узилишлар натижасида тизимда конфликтларнинг вужудга келиш имкониятини белгиловчи машина дастури.

### **Анализаторы сетевые**

**uz** - тармоқ анализа-

торлари

**en** - network analyzers

Программы, осуществляющие «прослушивание» сетевого трафика и автоматическое выделение из трафика имен пользователей, паролей, номеров кредитных карт и другой подобной информации.

Тармоқ трафикини «эшитишни» ва трафикдан автоматик равишда фойдаланувчилар номларининг, пароллар, кредит карточкалар рақамларининг ва бошқа шунга ўхшаш ахборотнинг ажратиб олинишини амалга оширадиган дастурлар.

### **Антивирус**

**uz** - антивирус

**en** - antivirus

Программа, предназначенная для защиты от вирусов, обнаружения зараженных программных модулей и системных областей, а также восстановления исходного состояния зараженных объектов.

## А

Вируслардан ҳимоя қилиш, зарарланган дастурий модуллар ва тизим соҳаларини аниқлаш, шунингдек, зарарланган объектларнинг бошланғич ҳолатини тиклаш учун мўлжалланган дастур.

### Аппаратура засекречивания

**uz** - махфийлаштириш аппаратураси  
**en** - cipheru equipment

Специальные технические устройства для автоматического шифрования и дешифрования телефонных и телеграфных переговоров (сообщений).

### Архивирование

**uz** - архивламоқ  
**en** - archiving

Хранение любых резервных файлов и любых обобщенных документов.

### Архивировать

**uz** - архивлаш  
**en** - to archive

Ҳар қандай резерв файллар ва умумлаштирилган ҳужжатларни сақлаш.

Хранить резервные файлы и любые взаимосвязанные с ними журналы, обычно в течение заданного периода времени.

Резерв файлларни ва улар билан ўзаро боғлиқ бўлган ҳар қандай журналларни, одатда белгиланган вақт даври мобайнида сақлаш.

### Атака

**uz** - ҳужум  
**en** - attack

1. Попытка нарушить компьютерную безопасность. Например, вредоносная программа, перехват.
2. Действие нарушителя, которое приводит к реализации угрозы путем использования уязвимостей автоматизированной системы.
3. Злонамеренные действия злоумышленника.
4. Попытка взлома защиты системы с целью перехвата информации, ее ком-

## А

прометации, нарушения режима сетевого обслуживания и т.д.

5. Попытка преодоления защиты системы. Атака может быть активной, ведущей к изменению данных или пассивной. Тот факт, что атака была осуществлена, не значит, что она успешна. Степень «успеха» атаки зависит от уязвимости системы и эффективности защитных мер.

1. Компьютер хавфсизлигини бузишга уриниш. Масалан, зарарли дастур, тутиб олиш.

2. Бузгунчи томонидан автоматлаштирилган тизим заифликларидан фойдаланиш йўли билан таҳдидни амалга ошириш ҳаракати.

3. Жинойткорнинг ёвуз ниятдаги ҳаракатлари.

4. Ахборотни қўлга киритиш, унга путур етказиш (обрўсизлантириш), тармоқ хизмати режимини бузиш ва б.қ. мақсадда тизим ҳимоясини бузишга уриниш.

5. Тизим ҳимоясини енгиб ўтишга уриниш. Хужум маълумотларни ўзгартиришга олиб келувчи актив ёки пассив бўлиши мумкин. Хужумнинг амалга оширилганлиги унинг муваффақиятини билдирмайди. Хужумнинг «муваффақият» даражаси тизим қанчалик заифлигига ва муҳофаза чораларининг самарадорлигига боғлиқ.

**Атака активная**  
**uz** - актив ҳужум  
**en** - active attack

Попытка проникновения в систему с изменением содержания передаваемой информации.

Тизимга, узатилаётган ахборотнинг мазмунини ўзгартириб, киришга уриниш.

**Атака аналитичес-**

Попытка разгадать код или найти ключ,

## А

**кая**

**uz** - аналитик хужум

**en** - analytical attack

используя аналитические методы. Например, статистический анализ изображений; поиск недостатков в алгоритме шифрования.

*Примечание: Противоположность атаки на основе полного перебора.*

Аналитик методлардан фойдаланиб, кодни билиб олишга ёки калитни топишга уриниш. Масалан, тасвирларнинг статистик тахлили; шифрлаш алгоритмидаги камчиликларни излаб топиш.

*Изоҳ: Тўлиқ ажратилиш асосидаги хужумнинг акси.*

**Атака внутренняя**

**uz** - ички хужум

**en** - insider attack

Атака, выполняемая из самой защищенной сети.

Муҳофазаланган тармоқнинг ўзидан амалга ошириладиган хужум.

**Атака перебором  
открытого текста**

**uz** - очик матнни тан-

лаш асосидаги хужум

**en** - chosen-plaintext

attack

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

Аналитик хужум, бунда криптоаналитик хабарнинг чекланмаган микдордаги очик матнларини кўриб чиқиши ва тегишли шифрланган матнни тадқиқ қилиши мумкин.

**Атака переполнения**

**uz** - тўлдириб юбо-

риш хужуми

**en** - flooding attack

(overflow)

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

Катта ҳажмдаги сохта трафикни кири-тиш ҳисобига тармоқ ускунасининг (маршрутизатор, коммутатор ва б.лар-

## А

### **Атака по известному открытому тексту**

**uz** - маълум очик  
матн бўйича хужум  
**en** - known-plaintext  
attack

### **Атака полным перебором, атака лобовая**

**uz** - тўлик танлаш  
асосидаги хужум,  
рўпарадан қилинган  
хужум  
**en** - exhaustive attack,  
brute-force attack

### **Атака с известным открытым сообщением**

**uz** - маълум очик хабар билан қилинадиган хужум  
**en** - known-plaintext  
attack

### **Атака с частой сменой пароля**

**uz** - паролни тез-тез ўзгартириш билан

нинг) сунъий равишда ўта юкланишни вужудга келтириш.

Аналитическая атака, когда криптоаналитик располагает шифротекстом и значительным количеством соответствующего ему открытого текста.

Аналитик хужум, бунда криптоаналитик шифрланган матн ва унга тегишли очик матннинг маълум миқдорига эга бўлади.

Попытка нарушить компьютерную безопасность методом проб и ошибок, перебирая возможные значения паролей или ключей.

*Примечание: Противоположность аналитической атаки.*

Синаб кўриш ва хатолар методи билан, пароль ва қалитларнинг мумкин бўлган қийматларини танлаб, компьютер хавфсизлигини бузишга уриниш.

*Изоҳ – Аналитик хужумнинг акси.*

Вид атаки, при которой злоумышленник имеет доступ к системе и ему известен текст передаваемого сообщения, который он может динамически изменять, пытаясь скрыть зашифрованный текст.

Хужум тури, бунда жинойатчи тизимга кира олади ва унга узатиладиган хабарнинг, у шифрланган матнни яширган ҳолда учун динамик ўзгартириши мумкин бўлган хабарнинг матни маълум бўлади.

Вид активной атаки на систему с многоуровневой защитой, во время которой злоумышленник использует чужие идентификационные данные, постоянно их



## А

қилинадиган хужум  
en - leapfrog attack

меняет, пытаюсь запутать следы, чтобы было невозможно определить, откуда поступил первый вызов.

**Атака только по шифротексту**  
uz - фақат шифрланган матн бўйича қилинадиган хужум  
en - cipher text-only attack

Аналитическая атака, когда криптоаналитик располагает только шифротекстом.

**Атрибут доступа**  
uz - фойдалана олиш атрибути  
en - access attribute

Аналитик хужум, бунда криптоаналитик фақат шифрланган матнга эга бўлади.

**Аттестат объекта защиты**  
uz - муҳофаза қилинадиган объект аттестати

Информационный элемент, связанный с объектом защиты и определяющий права доступа субъекта системы к этому объекту. Может принимать значение из заданного множества значений (как правило, «чтение», «запись» и «выполнение»).

Муҳофаза объекти билан боғланган ва шу объектдан тизим субъектининг фойдалана олиш ҳуқуқини белгиловчи ахборот элементи. Берилган кўлаб қийматлардан аҳамиятлисини қабул қилиши мумкин (одатда, «ўқиш», «ёзиш» ва «бажариш»).

Документ, выдаваемый органом по сертификации или другим специально уполномоченным органом, подтверждающим наличие на объекте защиты необходимых и достаточных условий

## А

en - protection object certificate

для выполнения установленных требований и норм эффективности защиты информации.

Сертификатлаш бўйича орган ёки муҳофаза қилинадиган объектда ахборотни муҳофаза қилишнинг белгиланган талаблари ва самарадорлик нормалари бажарилиши учун зарур ва етарли шарт-шароитлар мавжудлигини тасдиқлайдиган бошқа махсус ваколатланган орган томонидан бериладиган ҳужжат.

Аттестация

uz - аттестатлаш

en - attestation

Деятельность по подтверждению соответствия объекта информатики требованиям государственных стандартов, иных нормативных документов по защите информации, утвержденных государственными органами по сертификации в пределах их компетенции. Аттестация дает право владельцу объекта информатики обрабатывать информацию с уровнем секретности, соответствующим уровню безопасности информации.

Информатика объектининг давлат стандартлари талабларига, сертификатлаш бўйича давлат органлари томонидан, уларнинг ўз ваколатлари доирасида тасдиқланган ахборот муҳофазаси бўйича бошқа норматив ҳужжатлар талабларига мувофиқлигини тасдиқлаш бўйича фаолият. Аттестатлаш информатика объектининг эгасига ахборотни, ахборот хавфсизлиги даражасига мос келувчи махфийлик даражасида, қайта ишлаш ҳуқуқини беради.

Аттестация в области защиты инфор-

Деятельность по установлению соответствия комплекса организационно-техни-

## А

**мация**

**uz** - ахборотни муҳофаза қилиш соҳасида аттестатлаш  
**en** - attestation in the field of information security

**Аттестация испытательных лабораторий**

**uz** - синов лабораторияларини аттестатлаш  
**en** - testing laboratories attestation

**Аудит**

**uz** - аудит  
**en** - audit

ческих мероприятий по защите объекта или процесса требованиям по защите информации.

Объект ёки жараёни муҳофаза қилиш бўйича ташкилий-техник тадбирлар комплексининг ахборотни муҳофаза қилиш юзасидан қўйиладиган талабларга мувофиқлигини белгилаш билан боғлиқ фаолият.

Удостоверение компетентности испытательных лабораторий и их оснащённости, обеспечивающих проведение на должном техническом уровне всех предусмотренных нормативно-технической документацией испытаний закрепленных видов продукции и/или видов испытаний.

Синов лабораторияларининг компетентлигини ва уларнинг норматив-техник хужжатларда кўзда тутилган бириктирилган маҳсулот турлари синовларини ва ёки синовлар турларини тегишли техник даражада ўтказишни таъминловчи тарзда жиҳозланганлигини тасдиқлаш.

1. Процесс получения и анализа записей системного журнала (журнала аудита) с целью установления текущего состояния защищенности системы.

2. Автоматическая запись в журнале сведений о событиях, связанных с работой системы безопасности: входах пользователей, доступе к защищенной информации и др.

3. Экспертиза автоматизированной системы и всех ее составляющих с целью определения состояния безопасности системы, ее соответствия требованиям

## А

действующего законодательства и организационно-распорядительных документов организации.

1. Тизим муҳофазаланганлигининг кундалик ҳолатини белгилаш мақсадида тизим журнали (аудит журнали) ёзувларини олиш ва таҳлил қилиш жараёни.
2. Журналга хавфсизлик тизими иши билан боғлиқ ҳодисалар: фойдаланувчиларнинг кириши, муҳофазаланган ахборотдан фойдалана олиш ва б.лар ҳақидаги маълумотларни автоматик тарзда ёзиш.
3. Автоматлаштирилган тизим ва унинг барча ташкил этувчиларини, тизим хавфсизлигининг ҳолатини аниқлаш, унинг амалдаги қонунчилик талабларига ва ташкилотнинг ташкилий-идора қилиш ҳужжатларига мувофиқлигини аниқлаш мақсадида, экспертиза қилиш.

**Аудит безопасности**  
**uz - хавфсизлик ауди**  
**ти**  
**en - security audit**

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.

Тизимнинг бошқарувчи функцияларини адекватликка текшириш, қабул қилинган хавфсизлик сиёсати ва операцион процедураларга мувофиқлигини таъминлаш, хавфсизликнинг бузилишларини аниқлаш ҳамда бошқарувда, хавфсизлик сиёсатида ва процедураларда ҳар қандай муайян

## А

Ўзгаришлар бўйича тавсиялар бериш мақсадида, маълумотларни қайта ишлаш тизими ёзувларини ва унинг ишини мустақил кўриб чиқиш ва таҳлил қилиш.

### **Аудит компьютерной системы**

**uz** - компьютер

тизимнинг аудити

**en** - computer-system  
audit

Экспертиза процедур, используемых в системе обработки данных, для оценки их эффективности и правильности выполнения, а также выдача рекомендаций по повышению безопасности.

Маълумотларни қайта ишлаш тизимида қўлланиладиган процедураларни, уларнинг самарадорлиги ва тўғри бажарилаётганлигини баҳолаш юзасидан экспертиза қилиш, шунингдек, хавфсизликни ошириш бўйича тавсиялар бериш.

### **Аудитор безопасности**

**uz** - хавфсизлик аудитори

**en** - security auditor

Лицо или процесс, которому разрешен доступ к данным проверки безопасности и создание отчетов о проверке.

Хавфсизликни текширишга оид маълумотлардан фойдаланиш ва текширув тўғрисида ҳисоботлар тузиш рўхсат этилган шахс ёки жараён.

### **Аутентификатор**

**uz** - аутентификатор

**en** - authenticator

Средство аутентификации, представляющее отличительный признак пользователя.

*Примечание: Средствами аутентификации пользователя могут быть дополнительные кодовые слова, биометрические данные и другие отличительные признаки пользователя, которые вводятся в ЭВМ с клавиатуры дисплея, с идентификационной карты или при помощи специального устройства аутентификации по биометрическим данным.*

Фойдаланувчининг фарқловчи белгисини кўрсатувчи аутентификация воситаси.

## А

*Изоҳ: Қўшимча кодли сўзлар, биометрик маълумотлар ва фойдаланувчининг бошқа фарқловчи белгилари аутентификация воситалари бўлиши мумкин. Улар электрон ҳисоблаш машинасига дисплей клавиатурасидан, идентификацион картадан ёки биометрик маълумотларга қараб аутентификация қилишнинг махсус қурилмалари ёрдамида киритилади.*

**Аутентификация**  
**uz** - аутентификация  
қилиш  
**en** - authentication

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

Фойдаланувчининг (тармоқ абонентининг, хабар жўнатувчининг), дастур, қурилма ёки маълумотларнинг (ахборотнинг, олинадиган хабарнинг, калитнинг) ҳақиқийлигини белгилаш процедураси.

**Аутентификация**  
**взаимная**  
**uz** - ўзаро аутентификация қилиш  
**en** - mutual authentication

Процедура аутентификации, при которой осуществляется одновременно проверка регистрационных данных мобильной и базовой станций.

Аутентификация процедураси, унда мобил ва базавий станцияларнинг рўйхатдан ўтказиладиган маълумотларини текшириш бир вақтда амалга оширилади.

**Аутентификация**  
**данных**  
**uz** - маълумотларни аутентификация қилиш  
**en** - data authentication

Процесс проверки целостности данных. Например, проверка того, что полученные данные идентичны отправленным данным, а также проверка того, что программа не заражена вирусом.

Маълумотлар яхлитлигини текшириш жараёни. Масалан, олинган маълумот-

## А

ларнинг жўнатилган маълумотлар билан бир хиллигини, шунингдек, дастурда вирус бор ёки йўқлигини текшириш.

### **Аутентификация источника данных**

**uz** - маълумотлар манбаини аутентификация қилиш  
**en** - data origin authentication

Подтверждение подлинности источника полученных данных.

Олинган маълумотлар манбаининг ҳақиқийлигини тасдиқлаш.

### **Аутентификация личности**

**uz** - шахсни аутентификация қилиш  
**en** - identity authentication

Выполнение проверок, позволяющих системе обработки данных распознавать логические объекты. Например, проверка пароля или личного токена.

Маълумотларни қайта ишлаш тизимининг мантикий объектларни аниқлаб олиш имконини берадиган текширувларнинг бажарилиши. Масалан, пароль ёки шахсий токенни текшириш.

### **Аутентификация неявная**

**uz** - ноаниқ аутентификация  
**en** - implicit authentication

Процедура аутентификации, основанная на использовании ключей шифрования, которые генерируются по заданному алгоритму в процессе аутентификации.

Аутентификация қилиш жараёнида берилган алгоритм бўйича генерацияланадиган шифрлаш калитларидан фойдаланишга асосланган аутентификация қилиш процедураси.

### **Аутентификация односторонняя**

**uz** - бир томонлама аутентификация қилиш  
**en** - single-side authentication

Аутентификация отправителя или получателя сообщения.

Хабар жўнатувчи ёки олувчини аутентификация қилиш.

## А

### **Аутентификация сильная**

**uz** - кучли аутентификация  
**en** - strong authentication

Помимо проверки идентификатора и пароля пользователя, для осуществления процесса аутентификации используется криптографическое преобразование всей аутентифицируемой информации.

### **Аутентификация слабая**

**uz** - кучсиз аутентификация  
**en** - poor authentication

Проверка только идентификатора и пароля пользователя, иницилирующего процесс аутентификации.

### **Аутентификация сообщения**

**uz** - хабарни аутентификация қилиш  
**en** - message authentication

Аутентификация қилиш жараёнини амалга оширувчи фойдаланувчининг фақат идентификатори ва паролни текшириш.

### **Аутентификация явная**

**uz** - аниқ аутентификация  
**en** - explicit authentication

Процесс верификации идентификационной информации, предъявленной логическим объектом.

Мантикий объект томонидан тақдим этилган идентификацион ахборотни верификация қилиш жараёни.

Процедура аутентификации по паролю или с использованием заранее сформированных криптографических ключей, структура которых в процессе аутентификации не изменяется.

Пароль бўйича ёки структураси аутентификация қилиш жараёнида ўзгармайдиган, олдиндан шакллантирилган криптографик калитлардан фойдаланиб аутентификация қилиш жараёни.



## А

**Аутентичность**  
**uz** - ҳақиқийлик  
**en** - authenticity

Свойство данных быть подлинными или свойство систем быть способными обеспечить подлинность данных.

Маълумотларнинг ҳақиқий бўлиш хусусияти ёки тизимларнинг маълумотлар ҳақиқийлигини таъминлай олиш хусусияти.

## Б

**База вычислительная достоверная, ДВБ**  
**uz** - ишончли  
хисоблаш базаси,  
**ИХБ**  
**en** - Trusted Computing Base, TCB

Совокупность защитных механизмов вычислительной системы, включая программные и аппаратные компоненты, ответственные за поддержание политики безопасности.

Ҳисоблаш тизими муҳофаза механизмларининг жами, жумладан, хавфсизлик сифатини қўллаб-қувватлаш учун жавобгар дастурий ва аппарат компонентлар.

**База данных распределенная**  
**uz** - тақсимланган  
маълумотлар базаси  
**en** - distributed database

База данных физически распределенная на две или больше компьютерные системы.

Физик жиҳатдан икки ёки ундан ортик компьютер тизимларига тақсимланган маълумотлар базаси.

**База информационная**  
**uz** - ахборот базаси  
**en** - information base

Совокупность описания специальных объектов, существование которых в предметной области предусмотрено в конкретный момент времени или в определенный период времени, и описания текущих состояний связей, представляющих интерес в предметной области.

Предмет соҳасида мавжудлиги аниқ вақт онида ёки маълум вақт даврида кўзда тутилган махсус объектлар тавсифлари йиғиндиси, предмет соҳасида қизиқиш

## Б

уйғотувчи алоқалар жорий ҳолатининг тавсифи.

**Барьер информации**

**uz** - информация

тўсик

**en** - information barrier

Совокупность различных препятствий, возникающих на пути распространения и использования информации.

Ахборотни тарқатиш ва ундан фойдаланиш йўлида юзага келадиган турли тўсиклар.

**Барьер коммуникационный**

**uz** - коммуникацион

тўсик

**en** - communication barrier

Барьер, возникающий в процессе взаимодействия между системными аналитиками и управленческим персоналом предприятия (учреждения) при разработке и внедрении автоматизированных систем.

Автоматлаштирилган тизимларни ишлаб чиқиш ва жорий қилишда, ўзаро ҳамкорлик қилиш жараёнида тизим аналитиклари ва корхона (муассаса)нинг бошқарув персонали ўртасида юзага келадиган тўсик.

**Безопасность**

**uz** - хавфсизлик

**en** - security

1. Способность системы или сети обеспечивать защиту, достоверность и надежность хранения информации
2. Способность объекта противостоять воздействиям случайных и преднамеренных угроз.

1. Тизим ёки тармоқнинг, ахборотнинг муҳофаза қилинишини, ҳақиқийлигини ва ишончли сақланишини таъминлаш қобилияти.

2. Объектнинг тасодифий ва қасдан қилинадиган таҳдидлар таъсирига қарши тура олиш қобилияти.

**Безопасность автоматизированной**

Совокупность мер управления и контроля, защищающая автоматизированную

## Б

### **информационной системы**

**uz** - автоматлаштирилган ахборот тизимнинг хавфсизлиги  
**en** - automated information system security

### **Безопасность автоматизированной системы**

**uz** - автоматлаштирилган тизимнинг хавфсизлиги  
**en** - automated system security

### **Безопасность административная**

**uz** - маъмурий хавфсизлик  
**en** - administrative security

информационную систему от отказа в обслуживании и несанкционированного (умышленного или случайного) раскрытия, модификации или разрушения этой системы и данных.

Автоматлаштирилган ахборот тизимига хизмат кўрсатишдаги бузилиш ва бу тизимни ҳамда маълумотларни рухсат этилмаган тарзда (қасддан ёки тасодифан) очиш, ўзгартириш ёки бузишдан муҳофаза қилувчи бошқарув ва назорат чора-тадбирларининг жами.

Защищенность автоматизированной системы от несанкционированного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, незаконной модификации или разрушения ее компонентов.

Автоматлаштирилган тизимнинг, унинг нормал ишлаш жараёнига рухсат этилмаган аралашувдан, шунингдек, тизим компонентларини ўғирлаш, ноқонуний ўзгартириш ёки бузишдан муҳофаза қилинганлиги.

Административные меры, направленные на обеспечение компьютерной безопасности. К этим мерам относятся операционные процедуры и процедуры отчетности, процедуры расследования нарушений безопасности и анализ журналов аудита.

Компьютер хавфсизлигини таъминлашга қаратилган маъмурий чора-тадбирлар. Операцион процедуралар ва ҳисоб бериш процедуралари, хавфсизлик бузилишга

## Б

рини текшириш ҳамда аудит журналларини таҳлил қилиш процедуралари шундай чора-тадбирлар ҳисобланади.

### **Безопасность данных**

**uz** - маълумотларнинг хавфсизлиги  
**en** - data security

1. Компьютерная безопасность применительно к данным.
2. Защищенность данных от несанкционированных действий (случайных или умышленных), приводящих к модификации, раскрытию или разрушению данных.
3. Свойство системы противостоять попыткам несанкционированного доступа к обрабатываемой и хранимой информации.

1. Маълумотларга нисбатан қўлланиладиган компьютер хавфсизлиги.
2. Маълумотларнинг, маълумотлар ўзгартирилишига, фош бўлиш ёки бузилишига олиб келувчи, рухсат этилмаган таъсирлардан (тасодифий ёки қасддан) муҳофаза қилинганлиги.
3. Тизимнинг қайта ишланадиган ва сақланадиган ахборотдан рухсат этилмаган тарзда фойдаланиш йўлидаги уринишларга қарши тура олиш хусусияти.

### **Безопасность информации**

**uz** - ахборот хавфсизлиги  
**en** - information security

1. Защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.
2. Состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, иска-

## Б

жения, модификации (подделки), копирования, блокирования информации и т.п.

3. Защищенность устройств, процессов, программ, среды и данных, обеспечивающая целостность информации.

1. Ахборотнинг, номакбул (ахборот муносабатларининг тегишли субъектлари учун) ошкор қилинишдан (конфиденциаллигининг бузилишидан), ахборотнинг бузилиши ёки фойдалана олиш даражасини пасайишдан ёки йўқотилишдан, шунингдек, ноқонуний кўпайтирилишдан муҳофаза қилинганлиги.

2. Ахборотнинг, ахборот ресурсларининг ва ахборот тизимларининг ҳолати, унда талаб этиладиган эҳтимолликка кўра ахборотнинг (маълумотларни) тарқалиб кетишидан, ўғирлаш, йўқотиш, рухсат этилмаган тарзда ўчириш, бузиш, ўзгартириш (қалбакилаштириш), нусха кўчириш, блокировка қилиш ва ш.к. муҳофаза қилиш таъминланади.

3. Ахборотнинг яхлитлигини таъминловчи қурилмалар, жараёнлар, дастурлар, муҳит ва маълумотларнинг муҳофаза қилинганлиги.

**Безопасность информации (данных)**  
**uz** - ахборот (маълумотлар) хавфсизлиги  
**en** - security of information (data)

1. Интегральное свойство информации (данных) противостоять случайным или преднамеренным воздействиям (угрозам), наносящим ущерб собственнику информации. Характеристиками безопасности информации (данных) являются конфиденциальность, целостность и доступность.

2. Защищенность информации (данных) от несанкционированных случайных или умышленных действий, приводящих к утечке, подделке, копированию, модифи-

## Б

кации, раскрытию, разрушению, блокированию информации (данных).

3. Состояние защищенности информации (данных), обрабатываемых средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

1. Ахборот (маълумотлар)нинг ахборот эгасига зарар етказувчи тасодифий ёки қасддан қилинадиган таъсирлар (тахдидлар)га қарши тура олиш интеграл хусусияти. Конфиденциаллик, яхлитлик ва фойдалана олишлик ахборот (маълумотлар) хавфсизлигининг характеристикаси ҳисобланади.

2. Ахборот (маълумотлар)нинг ахборот (маълумотлар) тарқалиб кетишига, қалбақлаштирилишига, нусха кўчирилишига, ўзгартирилишига, фош бўлишига, бузилиши, блокировка қилинишига олиб келувчи, рухсат этилмаган тасодифий ёки қасддан бўладиган таъсирлардан муҳофаза қилинганлиги.

3. Ҳисоблаш техникаси ёки автоматлаштирилган тизим воситаларида қайта ишланадиган ахборот (маълумотлар)нинг ички ва ташқи таҳдидлардан муҳофазаланганлик ҳолати.

**Безопасность ин-  
формационная**  
**uz** - ахборот хавфсиз-  
лиги  
**en** - information  
security

1. Состояние защищенности интересов личности, общества и государства в информационной сфере.

2. Защита конфиденциальности, целостности и доступности информации.

3. Совокупность свойств информации и поддерживающей инфраструктуры быть защищенной от случайных или преднамеренных воздействий естественного или искусственного характера.

## Б

1. Ахборот соҳасида шахс, жамият ва давлат манфаатларининг муҳофаза қилинганлик ҳолати.
2. Ахборотнинг конфиденциаллигини, яхлитлигини ва ундан фойдалана олишликни муҳофаза қилиш.
3. Ахборот ва таъминловчи инфраструктуранинг табиий ёки сунъий характердаги тасодифий ёки қасддан қилинадиган таъсирлардан муҳофаза қилинганлик хусусиятларининг жами.

### Безопасность информационной системы

**uz** - ахборот тизими хавфсизлиги

**en** - information system security

1. Свойство информационной системы противостоять попыткам несанкционированного доступа.
2. Совокупность действий и мер, необходимых для обеспечения адекватной защиты системы, включая аппаратно-программные функции, характеристики и средства; операционные и учетные процедуры, средства управления доступом на сервере, удаленных компьютерах и средствах телекоммуникаций; административные мероприятия, физические конструкции и устройства; управление персоналом и коммуникациями системы.

1. Ахборот тизимининг рухсат этилмаган тарзда фойдаланишга уринишларга қарши тура олиш хусусияти.
2. Тизимнинг адекват муҳофазасини таъминлаш учун зарур бўлган амаллар ва чора-тадбирлар жами, жумладан, аппарат-дастурий функциялар, характеристикалар, воситалар; операцион ва ҳисобга олиш процедуралари, серверда, олисдаги компьютерлар ҳамда телекоммуникациялар воситаларида эркин фойдаланишни бошқариш воситалари; маъмурий тадбирлар, физик конструкциялар ва қурил-

## Б

- Безопасность информационно-технологии**  
**uz** - ахборот технологияси хавфсизлиги  
**en** - information technology security
- Безопасность коммуникационная**  
**uz** - коммуникацион хавфсизлик  
**en** - communications security, COMSEC
- Безопасность компьютерная**  
**uz** - компьютер хавфсизлиги  
**en** - computer security, COMPUSEC
- Безопасность многоуровневая**  
**uz** - кўп даражали хавфсизлик  
**en** - multilevel security
- малар; персонални ва тизим коммуникацияларини бошқариш.
- Защищенность технологического процесса обработки информации.
- Ахборотни қайта ишлаш технологик жараёнининг муҳофазаланганлиги.
- Защищенность коммуникаций (линий и каналов телекоммуникаций) от несанкционированного доступа.
- Коммуникацияларнинг (телекоммуникациялар линиялари ва каналларининг) рухсат этилмаган тарзда фойдаланишдан муҳофазаланганлиги.
- Свойство компьютерных систем противостоять попыткам несанкционированного доступа к обрабатываемой и хранимой информации, вводу информации, приводящей к деструктивным действиям, и навязыванию ложной информации.
- Компьютер тизимларининг қайта ишланадиган ва сақланадиган ахборотдан рухсат этилмаган тарзда фойдаланиш йўлидаги уринишларга, бузғунчилик ҳаракатларига олиб келувчи ахборотнинг киритилишига ҳамда сохта ахборот мажбуран киритилишига (қабул қилинишига) қарши тура олиш хусусияти.
- Класс систем, содержащих информацию с различными уровнями критичности.
- Критиклик даражаси турлича бўлган ахборотни ўз ичига олган тизимлар классси.



## Б

### **Безопасность операционная**

**uz** - операция хавфсизлик

**en** - operational data security

Защищенность данных от модификации, разрушения или разглашения (случайных, неавторизованных, либо преднамеренных) во время выполнения операций ввода, обработки или вывода.

Киритиш, қайта ишлаш ёки чиқариш операцияларини бажариш вақтида, маълумотларнинг ўзгартиришлардан, бузилишлардан ёки ошқор қилишлардан (тасодифий, муаллиф томонидан бўлмаган ёки қасдан) муҳофаза қилинганлиги.

### **Безопасность программного обеспечения**

**uz** - дастурий таъминот хавфсизлиги

**en** - software security

Свойство общецелевых (исполнительные программы, утилиты либо средства разработки программного обеспечения) и прикладных программ и средств осуществлять безопасную обработку данных в автоматизированной системе и безопасно использовать ресурсы системы.

Умуммақсадлардаги (бажарувчи дастурлар, утилиталар ёки дастурий таъминотни ишлаб чиқиш воситалари) ҳамда амалий дастур ва воситаларнинг автоматлаштирилган тизимда маълумотларнинг хавфсиз қайта ишланишини ва тизим ресурсларидан хавфсиз фойдаланишни амалга ошириш хусусияти.

### **Безопасность процедурная**

**uz** - процедуралар бўйича хавфсизлик

**en** - procedural security

Соответствующие способы управления, используемые с целью обеспечения требуемого уровня безопасности для критичных к защите информации данных.

Ахборотнинг муҳофаза қилинишига критик бўлган маълумотлар учун, талаб қилинадиган хавфсизлик даражасини таъминлаш мақсадида фойдаланиладиган тегишли бошқариш усуллари.

## Б

### **Безопасность реальной открытой системы**

**uz** - реал очик тизим хавфсизлиги  
**en** - real open system security

### **Безопасность ресурса автоматизированной системы**

**uz** - автоматлаштирилган тизим ресурсининг хавфсизлиги  
**en** - automatized system source security

Технологические и административные охраняемые меры, применяемые в реальной открытой системе для защиты оборудования, программного обеспечения и данных от случайных и преднамеренных модификаций, раскрытия и разрушения.

Ускуна, дастурий таъминот ва маълумотларни тасодифий ҳамда атайлаб қилинадиган ўзгартиришлардан, очиш ва бузишдан муҳофаза қилиш учун, реал очик тизимда қўлланиладиган технологик ва маъмурий ҳимоя чора-тадбирлари.

Безопасность ресурса автоматизированной системы складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности.

Конфиденциальность компонента системы заключается в том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

Целостность компонента предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права. Целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени.

Доступность компонента означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

Автоматлаштирилган тизим ресурсининг хавфсизлиги унинг учта характеристикасини: конфиденциаллигини, яхлитлигини

## Б

ва фойдалана олишликни таъминлашдан ташкил топади.

Тизим компонентининг конфиденциаллиги, унга фақат тегишли ваколати бўлган фойдалана олиш субъектлари (фойдаланувчилар, дастурлар, жараёнлар) кира олиши мумкинлигида ифодаланади.

Компонентнинг яхлитлиги у фақат тегишли ҳуқуқлари бўлган субъект томонидангина ўзгартирилиши мумкинлигини назарда тутди. Яхлитлик компонентнинг исталган вақт онда тўғрилиги (ўзгармаслиги, иш қобилияти)нинг қафолати ҳисобланади.

Компонентдан фойдалана олишлик тегишли ваколатга эга субъект исталган вақтда, ҳеч қандай муаммосиз тизим (ресурс)нинг зарур компонентидан фойдаланиш учун руҳсат олиши мумкинлигини билдиради.

**Безопасность сети**  
**uz** - тармоқ хавфсизлиги  
**en** - network security

Меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов. Безопасность информационной сети включает защиту оборудования, программного обеспечения, данных и персонала.

Ахборот тармоғини руҳсат этилмаган тарзда фойдаланишдан, нормал ишлашга тасодифий ёки қасдан бўладиган аралашувлардан, унинг компонентларини бузишга уринишлардан сақловчи чоратадбирлар. Ахборот тармоғининг хавфсизлиги ускуна, дастурий таъминот, маълумот ва персоналнинг муҳофазасини ўз ичига олади.

## Б

**Безопасность сети телекоммуникаций информационная**  
**uz** - телекоммуникациялар тармоғининг ахборот хавфсизлиги  
**en** - information security of telecommunications network

Состояние защищенности сети телекоммуникаций от определенного (заданного) множества случайных и преднамеренных воздействий нарушителей (угроз безопасности) на объекты сети, циркулирующие в них данные и информацию управления сетью с целью ознакомления с ними, искажения, уничтожения или блокирования в процессе передачи для дезорганизации процессов функционирования сети телекоммуникаций.

Телекоммуникациялар тармоғининг, бузгунчиларнинг тармоқ объектларига, уларда айланадиган маълумотларга ва тармоқни бошқариш ахборотига, улар билан танишиш, тузиб кўрсатиш, йўқ қилиш мақсадида бўладиган муайян (берилган) кўплаб тасодифий ва атайлаб қилинадиган таъсирларидан (хавфсизликка таҳдидларидан) ёки узатиш жараёнида телекоммуникациялар тармоғининг ишлаш жараёналарини издан чиқариш учун блокировка қилишдан муҳофаза қилинганлик ҳолати.

**Безопасность сети телекоммуникаций общего пользования информационная**  
**uz** - умумий фойдаланишдаги телекоммуникациялар тармоғининг ахборот хавфсизлиги  
**en** - public switched telecommunications network information security

Состояние (степень) защищенности информационных ресурсов сети телекоммуникаций общего пользования от угроз их информационной безопасности, приводящих к снижению заданного уровня качества служб или к ухудшению заданных качественных характеристик работы сети и, тем самым, к нанесению ущерба ее владельцам или пользователям.

Умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот ресурсларининг хизмат сифати даражасининг пайсишига ёки тармоқ иши сифат характеристикаларининг ёмонлашишига олиб

## Б

келувчи, шу билан унинг эгаси ёки фойдаланувчиларга зиён етказувчи тахдидлардан муҳофаза қилинганлик ҳолати (даражаси).

**Безопасность сети телекоммуникаций технологическая**  
**uz** - телекоммуникациялар тармоғининг технологик хавфсизлиги  
**en** - technological security of telecommunications network

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.

Телекоммуникациялар тармоғи аппаратдастурий таъминотининг кўпоровчилик типигаги жиноят-корона нуқсонларга, яъни маълум вақт ўтгандан сўнг ёки команда бўйича номақбул оқибатларга олиб келувчи ҳаракатни амалга оширишга қодир воситаларга эга бўлмаслик хусусияти.

**Безопасность субъектов информационных отношений**  
**uz** - ахборот муносабатлари субъектларининг хавфсизлиги  
**en** - information relation subjects security

Защищенность субъектов информационных отношений от нанесения им материального, морального или иного ущерба путем воздействия на информацию и/или средства ее обработки и передачи.

Ахборот муносабатлари субъектларининг уларга ахборот ва/ёки уни қайта ишлаш ва узатиш воситаларига таъсир этиш орқали моддий, маънавий ёки бошқа зарар етказилишдан муҳофаза қилинганлиги.

**Безопасность физической**  
**uz** - jismoniy хавфсизлик

Реализация физических барьеров и контрольных процедур, как превентивная или контрмера против физических угроз (взлома, кражи, террористического акта, а также

## Б

- en - physical security      пожара, наводнения и т.д.) ресурсам системы и критичной информации.
- Тизим ресурслари ва критик ахборотга жисмоний тахдидлар (бузиш, ўғирлаш, террорчилик акти, шунингдек ёнгин, сув тошқини ва б.к.)га қарши оғохлантирувчи ёки қарши чора каби жисмоний тўсиқлар ва назорат процедураларини амалга ошириш.
- Биометрия**  
uz - биометрия  
en - biometric
- Наука об использовании для идентификации личности биологических свойств, например, отпечатков пальцев или голоса.
- Шахсни идентификация қилиш учун биологик хусусиятлардан, масалан, бармоқ излари ёки овоздан фойдаланиш тўғрисидаги фан.
- Бит достоверности**  
uz - ишончлилиқ бити  
en - validity bit
- Разряд, добавляемый к слову в памяти ЭВМ для указания достоверности информации.
- ЭХМ хотирасидаги сўзга ахборотнинг ишончлилигини кўрсатиш учун кўшиладиган разряд.
- Бит защиты**  
uz - муҳофаза бити  
en - security bit
- Двоичный разряд в ключе памяти, устанавливающий защиту соответствующего блока памяти от записи либо от выборки и записи.
- Хотира қалитидаги тегишли хотира блокинг ёзишдан ёки танлаш ва ёзишдан муҳофа қилинишини белгиловчи иккилик заряд.
- Бит контроля по четности**  
uz - жуфтлик бўйича назорат бити
- Контрольный бит, добавляемый к данным для контроля их верности таким образом, чтобы сумма двоичных единиц, составляющих данные, включая и еди-

## Б

**en** - parity check bit,  
parity bit

ницу контрольного бита, всегда была четной или нечетной.

Маълумотларга, уларнинг ишончилиги-ни назорат қилиш учун маълумотларни ташкил этувчи иккилик бирликларнинг йиғиндиси, жумладан, назорат бити бирлиги, ҳар доим жуфт ёки тоқ бўладиган тарзда қўшиладиган назорат бити.

**Бит маски**  
**uz** - ниқоб бити  
**en** - mask bit

Сочетание битов, устанавливаемых в нулевое или единичное значение для разрешения либо запрета определенных операций либо для проверки или изменения содержимого поля.

Муайян операцияларга рухсат этиш ёки уларни таъқиқлаш ёки майдон ичидагини текшириш ё бўлмаса ўзгартириш учун ноль ёки бирлик қийматга ўрнатиладиган битлар йиғиндиси.

**Блок**  
**uz** - блок  
**en** - block

1. Совокупность данных, которые вводятся или выводятся одновременно.
2. Последовательность битов, имеющая фиксированную длину.

1. Бир вақтда киритиладиган ёки чиқариладиган маълумотлар жами.
2. Белгиланган узунликка эга бўлган битлар кетма-кетлиги.

**Блокирование**  
**uz** - блокировкалаш  
**en** - blocking

Использование специальных методов защиты данных или программного обеспечения от несанкционированного копирования.

Рухсат этилмаган тарзда нусха қўчиришга қарши маълумотлар ёки дастурий таъминотни муҳофаза қилишнинг махсус методларини қўллаш.

## Б

### **Блокирование информации**

**uz** - ахборотни блокировкалаш  
**en** - information blocking

1. Утрата информацией при ее обработке техническими средствами свойства доступности, выражающаяся в затруднении или прекращении санкционированного доступа к ней для проведения санкционированных операций по ознакомлению, документированию, модификации или уничтожению.

2. Искусственное затруднение доступа пользователей к информации, не связанное с ее уничтожением.

1. Техник воситалар билан қайта ишлашда ахборотдаги ундан фойдалана олиш хусусиятиниң йўқолиши: Танишиш, хужжатлаштириш, ўзгартириш ёки йўқ қилиш бўйича рухсат этилган операцияларни ўтказиш учун, ахборотдан рухсат этилган тарзда фойдаланишни қийинлашувида ёки тўхтатилишида ифодаланади.

2. Ахборотни йўқотиш билан боғлиқ бўлмаган ҳолда фойдаланувчиларнинг ахборотдан фойдалана олишларини сунъий равишда қийинлаштириш.

### **Блокирование логическое**

**uz** - мантикий блокировкалаш  
**en** - logical blocking

Блокирование, выполняемое в базах данных на логическом уровне.

Маълумотлар базаларида мантикий даражада бажариладиган блокировкалаш.

### **Блокирование передачи информации (данных)**

**uz** - ахборот (маълумотлар) узатилишини блокировкалаш  
**en** - data transmission blocking

Одно из нарушений из области безопасности информации, выражающееся в прекращении передачи или задержке информации на время, за которое она теряет ценность для пользователя.

Ахборот узатилишини тўхтатишда ёки вақтинча ушлаб туришда ифодаланидиган (бу вақтда у фойдаланувчи учун ўз қимматини йўқотади) ахборот хавфсизлиги соҳасидаги бузилишлардан бири.



## Б

### **Блокирование физического**

**uz** - физик блокировка  
калаш

**en** - physical blocking

### **Блокировка**

**uz** - блокировка

**en** - lock, locking

### **Блокировка данных**

**uz** - маълумотларни  
блокировка  
калаш

**en** - data interlock

### **Блокировка доступа к памяти**

**uz** - хотирага кира  
олишни блокировка-  
лаш

**en** - memory lockout

### **Блокировка записи в память**

**uz** - хотирага ёзишни  
блокировка  
калаш

**en** - memory write  
lockout

Блокирование, выполняемое в базах данных на физическом уровне.

Маълумотлар базаларида физик даражада бажариладиган блокировкакалаш.

Код, структура данных или программа для управления доступом к данным.

Маълумотлардан фойдалана олишни бошқариш учун мўлжалланган код, маълумотлар структураси ёки дастур.

Защита файла или его части (блока записи) путем запрещения доступа к ним всех пользователей, за исключением одного.

Битта фойдаланувчидан ташқари барча фойдаланувчиларга киришни таъқиқлаш йўли билан файл ёки унинг бир қисмини (ёзув блоқини) муҳофазалаш.

Запрещение доступа к ограниченному участку памяти, например, дорожке диска, вследствие обнаруженных на этом участке дефектов. Выполняется программными или аппаратными средствами.

Хотиранинг чекланган участкасига, масалан, диск йўлкасига, бу участкада аниқланган нуқсонлар оқибатида кира олишнинг таъқиқланиши. Дастурий ёки аппарат воситалар томонидан бажарилади.

Ситуация при обмене данными, характеризующаяся тем, что запись, читаемая с внешнего носителя, в основную память не переводится.

Маълумотлар алмашинишда вужудга келадиган вазият. Ташқи элтувчидан ўқи-

## Б

ладиган ёзув асосий хотирага кўчирил-маслиги билан тавсифланади.

### **Блокировка клавиатуры**

**uz** - клавиатурани

блокировкалаш

**en** - keyboard lockout

1. Запрет на ввод данных в ЭВМ с клавиатуры терминала. Выполняется операционной системой.

2. Игнорирование всех поступающих с клавиатуры сигналов и/или невозможность физического нажатия клавиш.

1. Маълумотларнинг терминал клавиатурасидан электрон ҳисоблаш машинасига киритилишини таъқиқлаш. Операцион тизим томонидан бажарилади.

2. Клавиатурадан келаётган барча сигналларнинг рад этилиши ва ёки клавишларни жисмоний босишнинг мумкин бўлмалиги.

### **Блокировка локальная**

**uz** - локал блокировкалаш

**en** - local lock

Блокировка с целью защиты ресурсов, приписанных к области, адресуемой отдельным пользователем.

Айрим фойдаланувчи томонидан йўлланаётган соҳага тегишли ресурсларни муҳофаза қилиш мақсадида блокировкалаш.

### **Блокировка учетной записи**

**uz** - ҳисобга оид ёзувни блокировкалаш

**en** - account lockout

Средство защиты пароля пользователя от подбора.

Фойдаланувчининг паролени саралашдан муҳофаза қилиш воситаси.

### **Блокнот одноразовый**

**uz** - бир мартали

блокнот

**en** - single-use pad

Криптосистема, также называемая шифром Вернама, использует строку бит, которая генерируется абсолютно случайно. Длина ключевого потока равна длине открытого текста и открытый текст и строка случайных бит комбинируются для выработки шифротекста, используя операцию XOR. Такой алгоритм обладает совершенной секретностью.

## Б

Вернам шифри деб ҳам аталадиган крипто-  
тотизим, мутлақо тасодифан генерация-  
ланадиган бит сатридан фойдаланади.  
Калит оқим узунлиги очик матн узунли-  
гига тенг. Тасодифий битлар сатри ва  
очик матн XOR операциясидан фойдала-  
ниб, шифр матнни ишлаб чиқиш учун  
комбинацияланади. Бундай алгоритм  
мутлақо махфий ҳисобланади.

### **Бомба временная**

**uz** - вақт бомбаси

**en** - time bomb

Логическая бомба, которая может быть  
активизирована в определенное время.

Муайян вақтда активлаштирилиши мум-  
кин бўлган мантикий бомба.

### **Бомба логическая**

**uz** - мантикий бомба

**en** - logic bomb

1. Вредоносная программа, запуск кото-  
рой происходит при некотором опреде-  
ленном состоянии системы обработки  
данных и вызывает повреждение этой  
системы.

2. Компьютерная программа или фрагмент  
программы, приводящая к повреждению  
ресурсов автоматизированной системы  
(данных, программного или аппаратного  
обеспечения) и срабатывающая при вы-  
полнении некоторого условия.

3. Программа ЭВМ, выполняемая перио-  
дически или в определенный момент  
времени с целью искажения, уничтоже-  
ния или модификации данных.

1. Маълумотларни қайта ишлаш тизими-  
нинг муайян бир ҳолатида ишга тушадиган  
ва тизимнинг ишдан чиқишига олиб  
келувчи зарарли дастур.

2. Автоматлаштирилган тизим ресурслар-  
рининг (маълумотлар, дастурий ёки ап-  
парат таъминот) шикастланишига олиб  
келувчи ва айрим шартлар бажарилганда

## Б

ишга тушадиган компьютер дастури ёки дастур фрагменти.

3. Маълумотларни бузиш, йўқ қилиш ёки ўзгартириш мақсадида, даврий равишда ёки муайян вақтда бажариладиган ЭХМ дастури.

### **Бомба почтовая**

**uz** - почта бомбаси

**en** - mail bomb

Блокирование сайта путем вывода из строя почтового сервера посылкой огромного числа писем. Используется для предотвращения получения сайтом писем в ходе атаки или для мести.

Сайтни, почта серверини кўп сонли хатларни юбориш орқали посилкаси билан ишдан чиқариш йўли билан блокировкалаш. Сайт орқали хужум чоғида хатлар олиншини бартараф қилиш ёки ўч олиш мақсадида ишлатилади.

### **Бомба программная**

**uz** - дастурий бомба

**en** - program bomb

Тайное встраивание в программу команд, которые должны срабатывать один или несколько раз при определенных условиях. *Примечание: Вариантами программной бомбы являются логическая и временная бомбы.*

Муайян шароитларда бир ёки бир неча марта ишга тушиши зарур бўлган командаларни дастурга яширин ўрнатиш.

*Изоҳ: Мантиқий ва вақт бомбалари дастурий бомбанинг вариантлари ҳисобланади.*

### **Брандмауэр**

**uz** - брандмауэр

**en** - firewall

Метод защиты сети от угроз безопасности, исходящих от других систем и сетей, с помощью централизации доступа к сети и контроля за ним аппаратно-программными средствами.

Тармокдан фойдалана олишни марказлаштириш ва аппарат-дастурий воситалар билан тармокни назорат қилиш ёрдамида бошқа тизимлар ва тармоқлардан

## Б

бўладиган хавфсизликка таҳдидлардан тармокни муҳофаза қилиш методи.

### **Брандмауэр с фильтрацией пакетов**

**uz** - пакетлар филтрацияланган брандмауэр

**en** - packet-filtering firewall

Маршрутизатор или компьютер, на котором работает программное обеспечение, сконфигурированное таким образом, чтобы отбраковывать определенные виды входящих и исходящих пакетов. Фильтрация пакетов осуществляется на основе информации, содержащейся в ТСП- и IP-заголовках пакетов (адреса отправителя и получателя, их номера портов и др.).

Кирувчи ва чикувчи пакетларнинг маълум бир турларини чиқариб ташлайдиган тарзда тузилган дастурий таъминот ишлайдиган маршрутизатор ёки компьютер. Пакетларни филтрлаш пакетларнинг ТСП ва IP сарлавҳаларида бўлган ахборот (жўнатувчи ва олувчининг адреслари, улар портларининг рақамлари ва б.) асосида амалга оширилади.

### **Брандмауэр экспертного уровня**

**uz** - эксперт даражадаги брандмауэр

**en** - stateful inspection firewall

Специальные алгоритмы фильтрации пакетов, с помощью которых каждый пакет сравнивается с известным шаблоном авторизованных пакетов. При этом проверяется содержимое принимаемых пакетов на трех уровнях модели ВОС: сетевом, сеансовом и прикладном.

Пакетларни филтрлашнинг махсус алгоритмлари. Улар ёрдамида ҳар бир пакет муаллифлаштирилган пакетларнинг маълум намунаси билан такқосланади. Қабул қилинадиган пакетларнинг ичидаги ВОС моделининг учта: тармок, сеанс ва амалий даражаларида текширилади.

## Б

**Брешь**  
**uz** - камчилик (заиф-  
лик)  
**en** - flaw

Ошибка при назначении полномочий, упущение при разработке, которые позволяют обойти или вывести из строя механизмы защиты.

Ваколатларни белгилашдаги, ишлаб чиқишдаги хато. Муҳофаза механизмларини четлаб ўтиш ёки уларни ишдан чиқариш имконини беради.

## В

**Вакцинирование**  
**uz** - вакциналаш  
**en** - inoculate

Запуск резидентных программ-вакцин, имитирующих сочетание условий, которые используются данным типом вируса для определения (выявления) заражения, то есть «обманывающих» вирус.

Берилган (маълум бир) вирус тури томонидан зарарланишни аниқлаш (топиш) учун фойдаланиладиган шарт-шароитларни имитацияловчи, яъни вирусни «алдайдиган» резидент вакцина дастурларни ишга тушириш.

**Ведение контроля**  
**uz** - назорат олиб бориш  
**en** - auditing

Отслеживание действий пользователей и запись операционной системой в контрольном журнале (security log) специальных типов событий, таких как регистрация в системе, доступ к файлу и т.п.

Фойдаланувчиларнинг ҳаракатларини кузатиб бориш ва операцион тизим томонидан назорат журналида (security log) тизимда қайд этиш, файлга кириш ва ш.к. ходисалар махсус турларининг ёзиб борилиши.

**Вектор аутентификационный**

Совокупность параметров, используемых при аутентификации мобильной станции,

## В

- uz** - аутентификацион вектор  
**en** - authentication vector
- напримеp, триплет в GSM и квинтет в UMTS.
- Мобил станцияни аутентификация қилишда қўлланиладиган параметрларнинг жами, масалан, GSM да триплет ва UMTS да квинтет.
- Вектор инициализации**  
**uz** - инициализация вектори  
**en** - initialization vector
- Случайное число, которое используется для инициализации процесса шифрования (не является секретным элементом).
- Величина контрольная криптографическая**  
**uz** - криптографик назорат катталиги  
**en** - cryptographic check value
- Шифрлаш жараёнини инициализациялаш учун қўлланиладиган тасодифий сон (махфий элемент ҳисобланмайди).
- Верификатор**  
**uz** - верификатор  
**en** - verifier
- Информация, получаемая в результате криптографического преобразования блока данных.
- Маълумотлар блоқини криптографик ўзгартириш натижасида олинадиган аҳборот.
- Объект, требующий аутентифицированной идентификации или представляющий его. Верификатор включает в себя функции, необходимые для осуществления обменов в целях аутентификации.
- Верификатор автоматический**  
**uz** - автоматик верификатор
- Аутентификацияланган идентификация қилиш талаб қилинадиган ёки уни кўрсатадиган объект. Верификатор аутентификация мақсадларида алмашинувларни амалга ошириш учун зарур бўлган функцияларни ўз ичига олади.
- Схема обеспечения автоматического доказательства правильности программ. Включает генератор условий верификаций и блок доказательства теорем.

## В

**en** - mechanical  
verifier

**Верификатор байт-кода**

**uz** - байт-код верификатори  
**en** - byte code verifier

Дастурларнинг тўғрилиги автоматик исботланишини таъминлаш схемаси. Верификациялар шартлари генератори ҳамда теоремаларни исботлаш блокани ичига олади.

Один из механизмов защиты модели безопасности технологии Java. Позволяет контролировать соответствие байт-кода Java спецификациям Java, приведение типов, переполнение стека и т.д.

Java технологияси хавфсизлик моделини муҳофаза қилиш механизмларидан бири. Java байт-кодининг Java спецификацияларига мувофиқлигини, типлар келтирилишини, стек тўлдирилишини ва ҳ.к. назорат қилиш имконини беради.

**Верификатор условий**

**uz** - шартлар верификатори  
**en** - assertion checker

Программа, анализирующая текст другой программы, снабженной условиями и операторами контроля, которые должны выполняться в определенных ее точках, и доказывающая их истинность либо ложность при заданных предусловиях.

Дастурнинг муайян нукталарида бажарилиши керак бўлган назорат шартлари ва операторлари билан таъминланган бошқа дастурнинг матнини таҳлил қилувчи ҳамда берилган шароитларда дастурларнинг ҳақиқийлигини исботловчи дастур.

**Верификация**  
**uz** - верификация  
**en** - verification

1. Сравнение работы, процесса или продукта с соответствующими требованиями либо спецификациями. Например, сравнение технических требований с моделью политики безопасности или сравнение кода объекта с исходным кодом.

2. Процесс сопоставления двух уровней спецификаций системы (например, моде-



## В

ли политики безопасности и спецификаций системы, спецификаций системы и исходных кодов, исходных кодов и выполняемых кодов) для установления необходимого соответствия между ними. Этот процесс может быть полностью или частично автоматизирован.

3. Установление соответствия, например, электронной подписи в принятом сообщении с имеющимся эталоном. Их совпадение свидетельствует о том, что целостность сообщения в процессе передачи не была нарушена.

1. Иш, жараён ёки маҳсулотни тегишти талаблар ёки спецификациялар билан таққослаш. Масалан, техник талабларни хавфсизлик сиёсати модели билан ёки объект коди ни дастлабки код билан таққослаш.

2. Тизим спецификацияларининг икки даражасини (масалан, хавфсизлик сиёсати модели ва тизим спецификациялари, дастлабки кодлар ва тизим спецификациялари ва дастлабки бажариладиган кодлар) улар ўртасида керакли мувофиқликни ўрнатиш учун таққослаш жараёни. Бу жараён тўлиқ ёки қисман автоматлаштирилиши мумкин.

3. Мувофиқликни, масалан, қабул қилинган хабардаги электрон имзонинг мавжуд эталон билан мувофиқлигини ўрнатиш.

**Верификация и  
утверждение  
uz - верификация ва  
тасдиқлаш  
en - verification and  
validation, V&V**

Полный набор проверок, которым подвергается система для получения гарантий ее соответствия своему назначению.

*Примечание: В число таких проверок могут входить жесткий набор функциональных тестов, контроль пропускной способности, проверка надежности и т.д.*

## В

Текширишларнинг тўла тўплами бўлиб, тизимнинг ўзи мўлжалланган мақсадларга мувофиқлигини кафолатлаш учун керак.

*Изоҳ: Функционал тестларни қатъий танлаш, ўтказиш, қобилиятини назорат қилиш, ишончлиликни текшириш ва ҳ.к. шундай текширишлар қаторига киради.*

### **Взлом**

**uz** - бузиш

**en** - hacking

Перехват начала сеанса связи, как правило, с целью осуществления активной атаки в момент, когда работающий в сети пользователь завершит аутентификацию. В этот момент злоумышленник пытается внедриться в систему как законный пользователь, что позволяет ему контролировать соединение между двумя станциями.

Тармоқда ишловчи фойдаланувчи аутентификацияни тугатганда, одатда, актив хужумни амалга ошириш мақсадида, алоқа сеансининг бошланишини тутиб олиш. Бу вақтда жинояткор тизимга конуний фойдаланувчи сифатида киришга ҳаракат қилади, бу унга иккита станция ўртасидаги уланишни назорат қилиш имконини беради.

### **Взлом, вскрытие криптосистемы**

**uz** - криптолизимни

бузиш, очиш

**en** - cryptosystem  
descrimination,

hacking

Создание процедуры, позволяющей вызывать отклонения информационного процесса, защищенного криптосистемой, от условий его нормального (штатного) протекания.

Криптолизим билан муҳофаза қилинган ахборот жараёнининг унинг нормал (штат) кечиш шароитларидан оғишини келтириб чиқариш имконини берадиган процедуранинг юзага келтириш.

### **Взломщик**

Лицо, предпринимающее попытку не-

## В

**uz** - бузувчи  
**en** - hacker

санкционированного проникновения в защищенную систему.

### **Взрыв**

**uz** - портлаш  
**en** - blowup

Муҳофазаланган тизимга рухсат этилмаган тарзда киришга уринувчи шахс.

В вычислительных системах - аварийный останов с выдачей сообщения об ошибке, блокирующий дальнейшее выполнение программы.

Ҳисоблаш тизимларида – хато тўғрисида хабар бериш билан, дастурнинг кейинчалик бажарилишига тўскинлик қиладиган авариявий тўхташ.

### **Взрыв комбинированный**

**uz** - комбинацияланган портлаш  
**en** - combined blowup

В интеллектуальных системах ситуация, когда размер пространства решений увеличивается чрезвычайно быстро с ростом числа элементарных решений. По этой причине метод перебора для поиска решения становится неприемлемым: необходимо использовать эвристические правила.

Интеллектуал тизимлардаги қарорларнинг фазовий ҳажми элементар қарорларнинг сони ўсиши билан фавқулодда тез кўпаядиган вазият. Шу сабабга кўра, ечим излаш учун ажратиш усули тўғри келмайди: эвристика қоидалардан фойдаланиш зарур.

**Вид активной атаки**  
**uz** - актив хужум тури  
**en** - active attack type

Внедрение злоумышленника между двумя системами для перехвата сообщений и подмены их собственными.

Икки тизим ўртасида, хабарларни тутиб олиш ва уларни шахсий хабарлар билан алмаштириш мақсадида, жинояткорни киритиш.

**Вид доступа**  
**uz** - фойдалана олиш

Вид операции, указанной в праве на доступ. Например, чтение, запись, выполнение.

## В

тури  
en - access type

ние, дополнение, модификация, удаление, создание.

Фойдалана олиш учун хукукда кўрсатилган операциялар тури. Масалан, ўқиш, ёзиш, бажариш, тўлдириш, ўзгартириш, ўчириш, яратиш.

**Вирус загрузочный**  
uz - юклаш вируси  
en - loading virus

Вирус, заражающий загрузочные части жестких и/или гибких дисков.

Қаттиқ ва ёки юмшоқ дискларнинг юкланадиган қисмларини зарарлайдиган вирус.

**Вирус (компьютерный)**  
uz - вирус  
en - virus

1. Анонимная программа, которая внедряется в вычислительную систему с целью исказить, модифицировать или уничтожить данные.

2. Программа, которая обладает следующими свойствами: возможностью копирования себя в другие файлы, диски, ЭВМ; возможностью выполнения без явного вызова; возможностью осуществления несанкционированного доступа к информации; возможностью маскировки от попыток обнаружения.

3. Вредоносная программа, способная создавать свои копии или другие вредоносные программы и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия.

1. Ҳисоблаш тизимига, маълумотларни бузиш, ўзгартириш ёки йўқ қилиш мақсадида киритиладиган аноним дастур.

2. Қуйидаги хусусиятларга: ўзини бошқа файлларга, дискка, ЭҲМга кўчириш; аниқ чақирувсиз бажариш; ахборотдан рухсат

## В

этилмаган тарзда фойдаланишни амалга ошириш; аниқлашга уринишдан маскировка қилиш имкониятига эга дастур.

3 Ўзининг нусхасини ёки бошқа зарарли дастурлар ярата оладиган ва уларни компьютер файлларига, тизим соҳаларига киритадиган, шунингдек, бошқа деструктив харакатларни амалга оширадиган зарарли дастур.

### **Вирус программный**

**uz** - дастур вируси

**en** - program virus

1. Программа, которая самопроизвольно размножается путем вставки своих возможно измененных копий в другие программы и модификации их при этом, и которая выполняется при вызове инфицированной программы.

2. Специально разработанная программа-вредитель, имеющая способность разрушать и видоизменять программное обеспечение системы.

1. Бошқа дастурларга ўзининг ўзгартирилган нусхаларини қўйиш йўли билан ўз-ўзидан кўпаядиган, уни ўзгартирадиган, зарарланган дастурни очишда амалга ошадиган дастур.

2. Тизим дастурий таъминотини бузиш ва кўринишини ўзгартирадиган, махсус ишлаб чиқилган зараркунанда дастур.

### **Вирусы-звенья**

**uz** - звено вируслар

**en** - unit viruses

Вирусы, не изменяющие код программы, а заставляющие операционную систему выполнить собственный код, изменяя адрес местоположения на диске зараженной программы на собственный адрес. После выполнения кода вируса управление обычно передается вызываемой пользователем программе.

Дастур кодини ўзгартирмайдиган, балки

## В

операцион тизимни зарарланган дастур дискида жойлашган адресни ўз адресига ўзгартирган ҳолда, ўзининг коди бажарилишига мажбур қиладиган вируслар. Вирус коди бажарилгандан сўнг, бошқариш одатда, фойдаланувчи томонидан чақирилладиган дастурга берилади.

### **Вирусы-компаньоны**

**uz** - компаньон вируслар

**en** - companion viruses

Эти вирусы создают свою копию на месте заражаемой программы, но не уничтожают оригинальный файл, а переименовывают или перемещают его. При запуске программы вначале выполняется код вируса, а затем управление передается оригинальной программе.

Нусхасини зарарланадиган дастур ўрнида яратадиган, оригинал файлни йўқ қилмасдан, уни қайта номлайдиган ёки силжитадиган вируслар. Дастурни ишга туширишда аввал вирус коди бажарилади, кейин бошқарув оригинал дастурга берилади.

### **Вирусы-мутанты**

**uz** - мутант вируслар

**en** - mutant viruses

Вирусы, которые содержат алгоритмы шифрования-расшифрования, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

Шифрлаш-расшифровкалаш алгоритмларини ичига олувчи вируслар. Бу алгоритмлар туфайли айнан бир вируснинг нусхалари байтларнинг бирорта ҳам такроланадиган занжирига эга бўлмайти.

### **Вирусы-невидимки**

**uz** - кўринмас вируслар

**en** - stealth viruses

1. Трудно обнаруживаемые и безвредные вирусы, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незара-

## В

женные участки диска.

2. Вирусы, использующие специальные алгоритмы, маскирующие их присутствие на диске, а в некоторых случаях и в оперативной памяти.

1 Аниқланиши ва зарарсизлантирилиши кийин бўлган вируслар, чунки улар операция тизимнинг зарарланган файлларга ва диск секторларига муружаатини тутиб олади ва ўз ўрнига дискнинг зарарланмаган участкаларини қўяди.

2. Ўзининг дискада, баъзи ҳолларда оператив хотирада мавжудлигини ниқобловчи махсус алгоритмлардан фойдаланадиган вируслар.

### **Вирусы неопасные**

**uz** - хавфли бўлмаган вируслар

**en** - harmless viruses

Вирусы, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках. Действия таких вирусов проявляются, как правило, в каких-либо графических или звуковых эффектах.

Компьютер ишига халакит бермайдиган, лекин бўш оператив хотира ва дисклардаги хотира ҳажмини камайтирадиган вируслар. Бундай вирусларнинг таъсири, одатда, қандайдир график ёки товуш эффектларида намоён бўлади.

### **Вирусы опасные**

**uz** - хавфли вируслар

**en** - harmful viruses

Вирусы, которые могут привести к различным нарушениям в работе компьютера.

Компьютер ишида турли бузилишларга олиб келиши мумкин бўлган вируслар.

### **Вирусы очень опасные**

**uz** - жуда хавфли вируслар

Вирусы, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

## В

en - herceluan viruses

Таъсир этиши дастурларнинг йўқотилишига, маълумотлар йўқ бўлишига, дискнинг тизим соҳаларида ахборот ўчиб кетишига олиб келиши мумкин бўлган вируслар.

**Вирусы паразитические**

uz - паразит вируслар

en - parasitic viruses

Все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, добавляя в них свой код, при этом оставляя сами файлы полностью или частично работоспособными.

*Примечание: Код вируса выполняется перед, после или вместе с программой, в зависимости от места внедрения вируса в программу.*

Нусхаларини тарқатишда файлга ўзининг кодини қўшган, файлларни тўлиқ ёки қисман ишлаш қобилиятини сақлаган ҳолда, файлларнинг ичидагини албатта ўзгартирадиган вируслар.

*Изоҳ: Вирус коди вирусни дастурга киритиш жойига боғлиқ равишда дастур олдидан, ундан кейин ёки дастур билан бирга бажарилади.*

**Вирусы перезаписывающие**

uz - қайта ёзадиган

вируслар

en - rewriting viruses

Вирусы, записывающие свое тело вместо кода программы, не изменяя названия исполняемого файла, вследствие чего исходная программа перестает запускаться. При запуске программы выполняется код вируса, а не сама программа.

Дастур коди ўрнига, бажариладиган файл номини ўзгартирмаган ҳолда, ўз жисмини ёзадиган вируслар. Бунинг оқибатида дастлабки дастурни ишга тушириш мумкин бўлмай қолади. Дастурни ишга туширишда дастурнинг ўзи эмас, балки вирус коди бажарилади.

**Вирусы полиморф-**

Вирусы, модифицирующие свой код в



## В

**ные**

**uz** - полиморф вирус-  
лар

**en** - polymorphic  
viruses

**Вирусы, поражаю-  
щие исходный код  
программ**

**uz** - дастурларнинг  
бошланғич кодини  
зарарлайдиган вирус-  
лар

**en** - viruses, attaching  
program initial code

**Вирусы простейшие**

**uz** - оддий вируслар  
**en** - simple viruses

**Вирусы резидент-  
ные**

**uz** - резидент вирус-  
лар

**en** - resident viruses

зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите.

Зарарланган дастурларда ўз кодини, айнан бир вируснинг иккита нусхаси бирорта ҳам битда мос тушмайдиган қилиб ўзгартирадиган вируслар.

Вирусы данного типа поражают или исходный код программы, либо её компоненты (OBJ-, LIB-, DCU- файлы), а также VCL и ActiveX компоненты. После компиляции программы оказываются в неё встроенными.

Дастурнинг бошланғич кодини ёки унинг компонентларини (OBJ-, LIB-, DCU-файлларни), шунингдек, VCL ҳамда ActiveX компонентларни зарарлайдиган вируслар. Компиляциядан сўнг дастурлар унга киритилган бўлади.

Вирусы, изменяющие содержимое файлов и секторов диска, которые могут быть достаточно легко обнаружены и уничтожены.

Файллар ва диск секторларининг ичидагини ўзгартирувчи, осон аниқланадиган ва йўқ қилинадиган вируслар.

Вирусы, оставляющие при заражении (инфицировании) компьютера в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т.п.) и внедряется в них. Эти вирусы находятся в памяти и остаются

## В

активными вплоть до выключения или перезагрузки компьютера.

Компьютерни зарарлашда оператив хотирада ўзининг резидент қисмини қолдирадиган вируслар. Бу резидент қисм операция тизимнинг зарарланган объектларга (файлларга, дискларнинг юклаш секторларига) муружаатини тутиб олади ва уларга қиради. Резидент вируслар хотирада бўлади ва компьютер ўчирилгунга ёки қайта юклангунга қадар активлигича қолади.

**Вирусы файловые**  
**uz** - файл вируслари  
**en** - file viruses

Вирусы, записывающие свой код в тело программного файла или документа, содержащего макрокоманды. При этом во время запуска программы (или загрузке документа для редактирования) эти вирусы получают управление.

*Примечание: По способу заражения файловые вирусы разделяют на перезаписывающие, паразитические, вирусы-звенья, вирусы-черви, компаньон-вирусы, а также вирусы, поражающие исходные тексты программ и компоненты программного обеспечения.*

Ўз кодини дастур файлига ёки макрокомандалар бўлган хужжатга ёзадиган вируслар. Дастурни ишга туширишда (ёки хужжатни тахрир қилиш учун юклашда) вируслар бошқарувга эга бўлади.

*Изоҳ: Зарарлаш усулига кўра файл вируслари қайта ёзадиган, паразит, звено вируслар, қурт вируслар, компаньон вирусларга, шунингдек, дастурларнинг дастлабки матнини ва дастурий таъминот компонентларини зарарловчи вирусларга ажратилади.*

**Владелец информации**  
**uz** - ахборот эгаси

1. Субъект, осуществляющий владение и пользование информацией и реализующий полномочия и распоряжения в пре-

## В

**en - information owner** делах прав, установленных законом и/или собственником информации.  
2. Субъект информационных отношений, обладающий правом владения, распоряжения и пользования информационным ресурсом по договору с собственником информации.

1. Ахборотга эгалик қилиш ва ундан фойдаланишни, қонун билан ва ёки ахборот эгаси томонидан белгиланган ҳуқуқлар доирасида ваколат ва фармойишларни амалга оширувчи субъект.

2. Ахборот муносабатларининг ахборот эгаси билан шартнома бўйича ахборот ресурсларига эгалик қилиш, фармойиш бериш ва ундан фойдаланиш ҳуқуқига эга субъекти.

**Владелец полномочия**

**uz -** ваколат эгаси

**en -** authority holder

Логический объект уровня, которому в данный момент присвоено полномочие.

Айни пайтда ваколат берилган, даражининг мантиқий объекти.

**Владелец сертификата**

**подписи**

**uz -** имзо сертификатининг эгаси

**en -** signature

certificate owner

Физическое или юридическое лицо, на имя которого выдан сертификат ключа подписи и которое владеет закрытым ключом ключа электронной цифровой подписи, соответствующим открытому ключу, указанному в сертификате.

Номига имзо қалитининг сертификати берилган, сертификатда кўрсатилган очик қалитга мос келувчи электрон рақамли имзо қалитининг ёпиқ қалитига эгалик қиладиган жисмоний ёки юридик шахс.

**Воздействие злонамеренное**

Действия, предпринимаемые в целях обхода механизмов обеспечения безопасности

## В

**uz** - ёмон ниятда қилинадиган таъсир  
**en** - attack

системы или в целях использования их недостатков.

*Примечания:*

1. При непосредственном злонамеренном воздействии на систему используются недостатки базовых алгоритмов, принципов или свойств механизма обеспечения безопасности.
2. Косвенные злонамеренные воздействия предпринимаются путем обхода механизма безопасности или принуждения системы к неправильному использованию этого механизма.

Тизимнинг хавфсизликни таъминлаш механизмларини четлаб ўтиш ёки уларнинг камчиликларидан фойдаланиш мақсадида амалга ошириладиган ҳаракат.

*Изоҳлар:*

1. Тизимга бевосита ёмон ниятда таъсир кўрсатилганда, базавий алгоритмларнинг хавфсизликни таъминлаш механизмнинг принциплари ёки хусусиятлари камчиликларидан фойдаланилади.

2. Билвосита ёмон ниятда қилинадиган таъсир хавфсизлик механизмини четлаб ўтиш ёки тизимни бу механизмдан нотўғри фойдаланишига мажбур қилиш орқали амалга оширилади.

**Воздействие на информационный ресурс внешнее**

**uz** - ахборот ресурсига кўрсатиладиган ташқи таъсир  
**en** - exposure on information resources

Фактор опасности, вызываемый стихийными бедствиями, мощными электромагнитными излучениями или диверсионными актами и приводящий к нарушению целостности информации либо ее блокированию.

Табийий офатлар, кучли электромагнит нурланишлар ёки қўпоровчилик ҳаракатлари келтириб чиқарадиган, ахборотнинг яхлитлиги бузилишига ёки унинг блокировка қилинишига олиб келадиган хавф омили.

**Воздействие на информацию непред-**

Ошибка пользователя, сбой технических и программных средств систем, природные

## В

**намеренное**

**uz** - ахборотга қасддан бўлмаган таъсир  
**en** - casual action on information

явления или иные не целенаправленные на изменение информации действия, приводящие к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Фойдаланувчининг хатоси, тизимнинг техник ва дастурий воситаларидаги носозлик, табиат ҳодисалари ёки ахборотнинг бузиб кўрсатилишига, йўқ қилинишига, ундан нусха олинмишига, ахборотдан фойдаланишнинг блокировка қилинишига, шунингдек, ахборот ташувчининг йўқолишига, йўқ қилинишига ёки ишлашида узилишлар келиб чиқишига олиб келадиган, бошқа мақсадга йўналтирилмаган, ахборотни ўзгартиришга бўлган ҳаракатлар.

**Воздействие на информацию несанкционированное**

**uz** - ахборотга рухсат этилмаган таъсир  
**en** - unauthorized action on information

Воздействие на защищаемую информацию с нарушением установленных прав и/или правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Муҳофаза қилинадиган ахборотга фойдаланишнинг белгиланган ҳуқуқлари ва ёки қоидаларини бузган ҳолда таъсир этиш. Бу ахборотнинг йўқолишига, бузиб кўрсатилишига, сохталаштирилишига, йўқ қилинишига, ахборотдан фойдаланишнинг блокировка қилинишига, шунингдек, ахборот ташувчининг йўқолишига, йўқ қилинишига ёки ишлашида узилишлар келиб чиқишига олиб келади.

## В

### **Воздействие с ретрансляцией злонамеренное**

**uz** - ретрансляция қилиш билан ёмон ниятда қилинадиган таъсир  
**en** - relay attack

### **Возможности недекларированные**

**uz** - декларация (эълон) қилинмаган имкониятлар  
**en** - undeclared capabilities

### **Воссоздание данных**

**uz** - маълумотларни янгитдан яратиш  
**en** - data reconstitution

### **Восстановление базы данных**

**uz** - маълумотлар базасини тиклаш

Злонамеренное воздействие на аутентификацию, при котором осуществляется перехват обмена аутентификационной информацией и немедленная ее ретрансляция.

Аутентификацияга ёмон ниятда таъсир кўрсатиш. Бунда аутентификацион ахборот алмашинуви тутиб олинди ва дарҳол ретрансляция қилинди.

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

Дастурий таъминотнинг баён қилинмаган ёки ҳужжатда баён қилинганларга мос келмайдиган функционал имкониятлари. Улардан фойдаланиш қайта ишланадиган ахборотнинг конфиденциаллиги, тушунарли бўлиши ёки яхлитлиги бузилишига олиб келиши мумкин.

Метод реставрации данных путем компоновки данных из частей доступных альтернативных источников.

Эркин фойдаланиш мумкин бўлган муқобил манбаларнинг қисмларини жой-жойига қўйиш йўли билан маълумотларни тиклаш методи.

1. Полная или частичная повторная загрузка базы данных.
2. Воссоздание содержимого базы данных по резервной копии, выполняемое в слу-

## В

**en** - database recovery

чае машинных сбоев или программных ошибок для поддержания целостности данных.

*Примечание: Методами и средствами восстановления являются копирование, рестарт с контрольной точки, системный журнал.*

1. Маълумотлар базасини тўлик ёки қисман такроран юклаш.
2. Маълумотлар базасини резерв нусхага қараб тиклаш. Маълумотларнинг яхлитлигини сақлаб туриш мақсадида машина бузилишлари ёки дастурий хатоликлар бўлган ҳолатларда бажарилади.

*Изоҳ: Нусха олиш, назорат нуқтасидан қайта бошлаш, тизим журнали тиклашнинг метод ва воситалари ҳисобланади.*

### Восстановление данных

**uz** - маълумотларни тиклаш

**en** - data recovery (reconstruction)

1. Приведение данных к предварительно известному или определенному состоянию.

2. Процесс копирования данных с носителя; содержащего защитную копию данных, на носитель-оригинал в случае нарушения на нем целостности данных.

1. Маълумотларни олдиндан маълум бўлган ёки муайян бир ҳолатга келтириш.

2. Маълумотларни, маълумотларнинг ҳимоя нусхаси бўлган ташувчидан оригинал ташувчига, маълумотлар яхлитлиги бузилган ҳолда, кўчириш.

### Восстановление обратное

**uz** - тесқари тиклаш

**en** - backward recovery

Использование более поздней версии данных, записанных в журнал, для воссоздания более ранней версии данных.

Маълумотларнинг журналга ёзилган охириги версиясидан маълумотларнинг дастлабки версиясини тиклашда фойдаланиш.

## В

**Восстановление после отказа**

**uz** - ишламай қолишдан сўнг тиклаш

**en** - failure recovery

Процедура возобновления работы вычислительной системы после отказа, исключая выработку системой неверных результатов.

Ҳисоблаш тизими ишини ишламай қолишдан сўнг тиклаш процедураси тизимнинг нотўғри натижалар чиқаришини истисно қилади.

**Восстановление при исчезновении питающего напряжения**

**uz** - таъминот кучланиши йўқолганда тиклаш

**en** - power fail recovery

Метод борьбы с последствиями отключения напряжения в питающей сети. Система оборудуется устройством контроля линии энергоснабжения, которое обнаруживает любое длительное отклонение напряжения в питающей сети за допустимые пределы и осуществляет прерывание по неисправности в системе питания, когда происходят такие отклонения. Программа обслуживания этого прерывания запоминает дескрипторы всех процессов в энергонезависимой памяти и затем останавливает работу. Когда напряжение в питающей сети восстанавливается, система снова запускается и может восстановить все процессы по их дескрипторам.

Таъминот манбаида кучланишнинг узилиб қолиш оқибатлари билан курашиш методи. Тизим электр таъминот линиясини назорат қилувчи қурилма билан жиҳозланади. Қурилма таъминот манбаидаги кучланишнинг йўл қўйиладиган чегарадан ҳар қандай четга чиқишини аниқлайди ва шундай четга чиқиш юз берганда, таъминот тизимида носозлик бўйича узилишни амалга оширади. Бу узилишга хизмат кўрсатиш дастурини энергияга боғлиқ хотирадаги барча жараёнларнинг дескрипторлари ёдда сақлай-



## В

ди, сўнг ишни тўхтатади. Таъминот манбаида кучланиш тикланганда, тизим яна ишга туширилади ва дескрипторлари бўйича барча жараёнларни тиклайди.

### Восстановление при ошибках

uz - хатолар бўлганда тиклаш

en - error recovery

Процесс исправления или обхода неисправности, позволяющий восстановить предписанное состояние системы.

Тизимнинг белгиланган ҳолатини тиклаш имкониятини берадиган, носозликни тузатиш ёки айланиб ўтиш жараёни.

### Восстановление прямое

uz - бевосита тиклаш

en - forward recovery

Использование более ранней версии данных, записанных в журнал, для воссоздания более поздней версии данных.

Маълумотларнинг журналга ёзилган дастлабки версиясидан маълумотларнинг охириги версиясини тиклашда фойдаланиш.

### Восстановление сети

uz - тармоқни тиклаш

en - network recovery

Совокупность действий, выполняемых для восстановления работоспособности вычислительной сети.

Ҳисоблаш тармоғининг ишлаш қобилиятини тиклаш мақсадида бажариладиган амаллар жами.

### Восстановление файла

uz - файлни тиклаш

en - file recovery

Процесс восстановления целостности файла после обнаружения в нем ошибок.

Хатоликлар аниқлангандан сўнг файлинг яхлитлигини тиклаш жараёни.

### Время безопасное

uz - хавфсиз вақт

en - security time

Математическое ожидание времени раскрытия системы защиты статистическим апробированием возможных вариантов доступа к данным.

## В

Маълумотлардан фойдаланишнинг мумкин бўлган вариантларини статистик си-наш орқали муҳофаза тизимининг очи-лиш вақтини математик кутиш.

### **Время восстановления**

**uz** - тиклаш вақти  
**en** - recovery time

Время между моментом обнаружения сбоя и моментом возобновления работы системы (устройства) после восстановления.

Носозлик аниқланган пайт билан тик-лашдан кейин тизим (қурилма) иши қайта тикланган пайт орасидаги вақт.

### **Время доступа (обращения)**

**uz** - фойдалана олиш  
(мурожаат қилиш)  
вақти  
**en** - access time

Интервал времени между моментом вы-дачи команды на ввод-вывод данных и моментом начала обмена.

Маълумотларни киритиш-чиқаришга ко-манда бериш пайти билан алмашиниш-нинг бошланиш пайти орасидаги вақт ин-тервали.

### **Время жизни**

**uz** - яшаш вақти  
**en** - life time

Интервал выполнения программы, в кото-ром программный объект (например, пере-менная) сохраняет свое значение.

Дастур объекти (масалан, ўзгарувчи) ўз ахамиятини сақлаб турадиган, дастурнинг бажарилиш интервали.

### **Время ремонта**

**uz** - таъмирлаш вақти  
**en** - repair time

Время (иногда среднее), необходимое для диагностирования и устранения непола-док либо в технических средствах, либо в программном обеспечении вычислитель-ной системы.

Техник воситалардаги ёки ҳисоблаш ти-зимининг дастурий таъминотидаги но-созликларни аниқлаш ва бартараф қилиш учун зарур бўлган (баъзида ўртача) вақт.

## В

**Вскрываеть паролей**

**uz** - паролларни очувчи  
**en** - password discriminator

**Вход (в систему)**

**uz** - кириш (тизимга кириш)  
**en** - logon

**Вход между строк**

**uz** - сатрлар орасига кириш  
**en** - between lines entry

**Вызов обратный**

**uz** - қайта чакирув  
**en** - call-back

Программа, осуществляющая подбор и обнаружение паролей.

Паролларнинг танланишини ва аникланишини амалга оширувчи дастур.

Предоставление пользователем идентифицирующих его сведений (например, имени, домена и пароля), проверка подлинности и образование сеанса работы пользователем.

Фойдаланувчи томонидан уни идентификация қилувчи маълумотларнинг (масалан, номи, домени ва пароли) такдим этилиши, ҳақиқийликни текшириш ва фойдаланувчининг иш сеансини ташкил қилиш.

Доступ, полученный нарушителем посредством активного перехвата при кратковременном выключении канала передачи данных, связанного с ресурсами законного пользователя.

Қонуний фойдаланувчининг ресурслари билан боғлиқ бўлган, маълумотлар узатиш каналини қисқа вақтга ўчириш пайтида бузгунчи томонидан актив тутиб олиш воситасида олинган кириш ҳуқуқи.

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.

Чакирувчи терминални аутентификация қилиш учун мўлжалланган процедура:

## В

дастлаб маълумотларни қайта тиклаш тизими чакирувчи терминални идентификация қилади, кейин чакирувнинг узилиши юз беради, сўнгра чакирувчи терминал раками терилади.

### **Вызов-ответ**

**uz** - чакирув-жавоб

**en** - challenge-response

Механизм проверки пароля. Сервер передает клиенту «вызов», тот преобразует его с помощью пароля и результат передает серверу как «ответ». Сервер проверяет, что «ответ» получен из «вызова» при помощи правильного пароля.

Паролни текшириш механизми. Сервер мижозга «чакирув»ни узатади, у пароль ёрдамида уни қайта ўзгартиради ва натижани серверга «жавоб» сифатида узатади. Сервер «жавоб» «чакирув»дан тўғри пароль ёрдамида олинганлигини текширади.

### **Вызов санкционированный**

**uz** - рухсат этилган

чакирув

**en** - authorized call

Вызов системы, программы или данных, разрешенный данному пользователю. Как правило, реализуется путем ввода и проверки пароля.

Белгиланган (маълум) фойдаланувчига рухсат этилган тизимни, дастур ёки маълумотларни чакириш. Одатда, паролни киритиш ва уни текшириш орқали бажарилади.

### **Выравнивание сектора**

**uz** - секторни

тўғрилаш

**en** - sector alignment

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

Нусха кўчиришдан муҳофаза қилиш методи, секторларнинг йўлқадан йўлкага тўғри ўрнатилганлигини текширишда

## В

диск рухсат этилмаган нухса бўлиб хисобланиши ёки ҳисобланмаслигини аниқлаш имконини беради.

## Г

**Гамма криптостой-  
кая**

**uz** - криптобардошли  
гамма

**en** - strong gamma

Гамма, по известному фрагменту которой нельзя определить другие ее фрагменты и восстановить со всеми деталями алгоритм, использованный для ее выработки.

Маълум фрагментга қараб, унинг бошқа фрагментларини аниқлаш ва уни ишлаб чиқиш учун фойдаланилган алгоритмни барча деталлари билан тиклаш мумкин бўлмаган гамма.

**Гамма шифра**

**uz** - шифр гаммаси

**en** - key stream,  
gamma of the cipher

1. Псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму, для зашифрования и расшифрования данных.

2. Псевдослучайная последовательность элементов данных, вырабатываемая по заданному алгоритму и используемая для зашифрования открытых данных и расшифрования зашифрованных данных путем комбинирования с ними обратимой бинарной операции.

1. Маълумотларни шифрлаш ва расшифровка қилиш учун берилган алгоритм бўйича ишлаб чиқиладиган псевдотасодифий иккилик кетма-кетлик.

2. Берилган алгоритм бўйича ишлаб чиқиладиган ва очиқ маълумотларни шифрлаш ҳамда қайтар бинар операцияни комбинациялаш йўли билан шифрланган маълумотларни расшифровка қилиш учун фойдаланиладиган, маълумотлар элементларининг псевдотасодифий кетма-кетлиги.

## Г

### **Гаммирование**

**uz** - гаммалаш

**en** - gamming

Процесс наложения по определенному алгоритму гаммы шифра на открытый текст.

Маълум алгоритми бўйича шифр гаммасини очик матнга қўйиш жараёни.

### **Гарантированность механизмов защиты информации**

**uz** - ахборотни

муҳофаза қилиш механизмларининг ка-

фолатланганлиги

**en** - information defence mechanism security

Оценка адекватности используемых механизмов защиты информации выбранным функциональным требованиям.  
*Примечание: Гарантированность определяется эффективностью и корректностью механизмов защиты информации.*

Фойдаланиладиган ахборотни муҳофаза қилиш механизмларининг танланган функционал талабларга адекватлигини (мослигини) баҳолаш.

*Изоҳ: Кафолатланганлик ахборотни муҳофаза қилиш механизмларининг самарадорлиги ва тўғрилиги билан аниқланади.*

### **Гарантия**

**uz** - кафолат

**en** - assurance

Мера доверия архитектуре и средствам обеспечения безопасности системы относительно корректности и аккуратности проведения политики безопасности.

Хавфсизлик сиёсатини ўтказишнинг тўғрилиги ва батартиблигига нисбатан архитектура ва тизим хавфсизлигини таъминлаш воситаларига ишонч ўлчови.

### **Генератор ключевого потока**

**uz** - калит оқими генератори

**en** - key stream generator

Алгоритм, вырабатывающий ключевой поток для потоковых криптосистем. Может быть либо детерминированным, чтобы воспроизвести одинаковый ключевой поток на концах отправителя и получателя, либо случайным. Если генератор детерминированный, то он зависит от секретного ключа. Генераторы ключевого потока обычно базируются на комбина-

## Г

циях регистров сдвига и нелинейных булевых функциях. При построении генераторов ключевого потока часто используют криптографические преобразования блочных шифров, например OFB или счетчиковый метод.

Оқимли криптолизимлар учун калит оқимини ишлаб чиқувчи алгоритм. Ё жўнатувчи ва олувчи учларида бир хил калит оқимини қайта ишлаб чиқиш учун детерминланган, ё тасодифий бўлиши мумкин. Агар генератор детерминланган бўлса, у махфий калитга боғлиқ бўлади. Калит оқими генераторлари одатда силжиш регистрларининг комбинациясига ва ночизикли Буль функцияларига асосланади. Калит оқими генераторларини тузишда, кўпинча, блокли шифрларни криптографик қайта тузишдан, масалан, OFB ёки ҳисоблагичли методдан фойдаланилади.

### **Генератор случайных паролей**

**uz** - тасодифий пароллар генератори  
**en** - randompassword generator

Программно-аппаратное средство, представляющее собой генератор случайных чисел, используемых в качестве паролей.

Пароллар сифатида фойдаланиладиган тасодифий сонлар генераторини ўзида ифодалайдиган дастурий-аппарат восита.

### **Генерация ключей**

**uz** - калитлар генерацияси

**en** - key generation

Процесс генерации криптографических ключей. Согласно правилу Кирхгоффа, стойкость криптографического алгоритма базируется на секретности ключа, поэтому генерация ключей – очень важный процесс, для выполнения которого используются различные методы, например, генераторы случайных и псевдослучайных последовательностей.

## Г

Криптографик калитларни генерациялаш жараёни. Кирхгофф коидасига мувофиқ, криптографик алгоритмнинг ўзгармаслиги калитнинг махфийлигига асосланади, шунинг учун калитлар генерацияси жуда муҳим жараён ҳисобланади, уни бажариш учун турли методлардан, масалан, тасодикий ва псевдотасодикий кетма-кетликдаги генераторлардан фойдаланилади.

### **Граница кодирования**

**uz** - кодлаш чегараси  
**en** - coding bound

Предел производительности кода, зависящий от таких параметров, как мощность кода, минимальное расстояние Хемминга, длина кодовой комбинации.

Код унумдорлигининг чегараси, у код куввати, минимал Хемминг масофаси, кодли комбинация узунлиги каби параметрларга боғлиқ.

### **Гриф секретности**

**uz** - махфийлик грифи  
**en** - security classification

1. Определенный уровень, который необходим в данном конкретном случае для защиты данных или информации от несанкционированного доступа вместе с указанием этого уровня. Например, «совершенно секретно», «секретно», «конфиденциально».
2. Надпись (штамп) на документе или издании, определяющая особый порядок пользования этим документом.
3. Специальная отметка на носителе информации, свидетельствующая о степени конфиденциальности информации, хранящейся на этом носителе.
4. Реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.



## Г

1. Берилган муайян ҳолатда маълумотлар ёки ахборотни рухсат этилмаган тарзда фойдаланишдан муҳофаза қилиш учун зарур бўлган аниқ белгиланган даража. Масалан, «мутлақо махфий», «махфий», «конфиденциал».
2. Хужжат ёки нашрдаги шу хужжатдан фойдаланишнинг муҳим тартибини белгиловчи ёзув (тамға).
3. Ахборот ташувчидаги шу ташувчида сақланадиган ахборотнинг конфиденциаллик даражасини тасдиқловчи махсус белги.
4. Ташувчининг ўзига ва (ёки) унга илова қилинадиган хужжатларга қўйиладиган, уларнинг элтувчиларида мавжуд бўлган маълумотларнинг махфийлик даражасини тасдиқловчи реқвизитлар.

## Д

**Дайджест**  
uz - дайжест  
en - digest

Код фиксированной длины, образующийся в результате обработки с помощью хэш-функции входного потока данных переменной длины. Так, например, алгоритм хэширования SHA-1 создает дайджест размером 20 bit, независимо от размера входного сообщения.

Ўзгарувчан узунликдаги маълумотларнинг кириш оқимини хэш-функция ёрдамида қайта ишлаш натижасида ҳосил бўладиган, қатъий узунликдаги код. Масалан, SHA-1 хэшлаш алгоритми кириш хабарининг ҳажмидан қатъи назар, 20 bit ҳажмидаги дайжестни яратади.

**Данные**  
uz - маълумотлар  
en - data

Информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека.

## Д

Одамнинг иштироки мумкин бўлган ҳолда, автоматик воситалар ёрдамида, қайта ишлаш учун ярқли кўринишда тақдим этилган ахборот.

### Данные биометрические

**uz** - биометрик маълумотлар  
**en** - biometric data

Средства аутентификации, представляющие собой такие персональные отличительные признаки пользователя как тембр голоса, форма кисти руки, отпечатки пальцев и т.д., оригиналы которых в цифровом виде хранятся в памяти ЭВМ.

Фойдаланувчининг, оригиналлари рақамли кўринишда ЭХМ хотирасида сақланадиган, овоз тембри, қўл бармоқларининг шакли, изи ва ш.к., шахсий фарқловчи белгиларини ўзида ифодаловчи аутентификация қилиш воситалари.

### Данные верительные

**uz** - ишонч маълумотлари  
**en** - credentials

Данные, передаваемые для установления заявленной подлинности логического объекта.

Мантиқий объектнинг қайд қилинган ҳақиқийлигини белгилаш учун узатиладиган маълумотлар.

### Данные закрытые (защищенные)

**uz** - ёпик (муҳофазаланган) маълумотлар  
**en** - private data

Данные, доступные ограниченному кругу пользователей. Как правило, ограничение доступа осуществляется системой паролей.

Фойдаланувчиларнинг тор доирасига мўлжалланган маълумотлар. Қоидага кўра эркин фойдаланишнинг чекланиши пароллар тизими орқали амалга оширилади.

### Данные зашифрованные

**uz** - шифрланган маълумотлар  
**en** - cipher data

Информация, хранящаяся в памяти ЭВМ в зашифрованном виде, т.е. данные, к которым применен способ криптографической защиты.

## Д

Электрон хисоблаш машинасида шифрланган кўринишда сақланадиган ахборот, яъни криптографик муҳофаза қилиш усуллари қўлланилган маълумотлар.

### **Данные персональные**

**uz** - шахсий маълумотлар  
**en** - personal data

1. Сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

2. Зафиксированная на любом материальном носителе информация о конкретном человеке.

1. Фуқаронинг шахсини идентификация қилиш имконини берувчи далиллар, воқеалар ва ҳаёт шароитлари ҳақидаги маълумотлар.

2. Ҳар қандай моддий ташувчида қайд этилган муайян одам тўғрисидаги маълумот.

### **Данные проверки безопасности**

**uz** - хавфсизликни текшириш маълумотлари  
**en** - security audit trail

Данные, которые собраны и могут быть использованы для содействия проведению проверки безопасности.

Хавфсизликни текширишга кўмаклашиш мақсадида тўпланган ва фойдаланилиши мумкин бўлган маълумотлар.

### **Данные с защитой целостности**

**uz** - яхлитлиги муҳофазаланган маълумотлар  
**en** - integrity-protected data

Данные и все соответствующие атрибуты в среде с защитой целостности.

Яхлитлик муҳофазаланган муҳитдаги маълумотлар ва барча тегишли атрибутлар.

### **Данные секретные**

**uz** - махфий маълумотлар

**en** - confidential data

Закрывые данные, которым присвоен определенный гриф (степень) секретности.

Маълум бир махфийлик грифи (даражаси) берилган ёпиқ маълумотлар.

## Д

### Данные теста

**uz** - тест маълумотлари

**en** - test data

Данные, используемые для контрольной задачи.

Назорат иши учун фойдаланиладиган маълумотлар.

### Дата и время изменения файла

**uz** - файл ўзгартирилган сана ва вақт

**en** - data and time stamp

Автоматическая фиксация в заголовке указателя файла даты и времени его создания или последней модификации.

Файл кўрсаткичидаги сарлавҳада уни яратиш ёки охирги ўзгартириш санаси ҳамда вақтини автоматик тарзда қайд этиш.

### Действие несанкционированное

**uz** - рухсатсиз

ҳаракат

**en** - unauthorized action

Действие субъекта в нарушение установленных в системе правил обработки информации.

Субъектнинг ахборотни қайта ишлаш тизимида белгиланган қоидаларни бузган ҳолда ҳаракат қилиши.

### Действия пользователя «скрытые»

**uz** - фойдаланувчининг «яширин»

ҳаракатлари

**en** - «convert» user action

Иные, отличные от «явных», действия, осуществляемые пользователем, в том числе с использованием собственных программ работы с устройствами.

«Ошкор» ҳаракатлардан фарқ қилувчи, фойдаланувчи томонидан, жумладан, қурилмалар билан ишлаш бўйича ўз дастурларидан фойдаланиб, амалга ошириладиган ҳаракатлар.

### Действия пользователя «явные»

**uz** - фойдаланувчининг «очик»

ҳаракатлари

**en** - «explicit» user action

Действия, осуществляемые пользователем, с использованием системных средств.

Фойдаланувчи томонидан тизим воситаларидан фойдаланиб амалга ошириладиган ҳаракатлар.

## Д

**Делегирование**  
**uz** - вакил қилиш  
**en** - delegation

Передача полномочия от одного объекта, который владеет данным полномочием, другому объекту.

**Демон**  
**uz** - демон  
**en** - demon

Ваколатни маълум ваколатга эга бўлган объектдан бошқа объектга бериш.

Программа, которая незаметно контролирует работу другой программы и время от времени прерывает ее работу, не разрушая саму программу (чаще всего это программа управления периферийными устройствами).

**Депонирование**  
**ключей**  
**uz** - калитларни сақлаш  
учун топшириш  
**en** - key escrow

Бошқа дастурнинг ишини сездирмай назорат қиладиган ва вақт-вақти билан дастурни (кўпинча бу периферик (ташқи) курилмаларни бошқариш дастури), унинг ишини бузмасдан тўхтатадиган дастур.

Процесс депонирования ключей, заключающийся в разбиении криптографического ключа на две части, каждая из которых шифруется и передается на хранение доверенным правительственным организациям, обеспечивающим надежное хранение ключевых компонентов в течение срока их действия. Эти компоненты позволяют службам, отвечающим за национальную безопасность, восстанавливать уникальные ключи и выполнять расшифрование сообщений.

Криптографик калитларни икки қисмга ажратиб, калитларни сақлаш учун топшириш жараёни, уларнинг ҳар бири шифрланади ва калит компонентлари амал қилиш муддати давомида ишончли сақлашни таъминловчи ишончли ҳукумат ташкилотларига сақлаш учун топширилади. Бу компонентлар миллий хавфсиз-

## Д

лик учун жавобгар хизматларга ноёб калитларни тиклаш ва хабарларни дастлабки матнга ўгириш имконини беради.

**«Дерево» Меркля**  
**uz** - Меркл «дарахти»  
**en** - Merkle's tree

Схема цифровой подписи, базирующаяся на одноразовых сигнатурах и хэш-функции. Применяется для устранения недостатков схемы одноразовых подписей. Позволяет отказаться от генерации ключевой пары для каждого нового сообщения.

Бир мартали сигнатуралар ва хэш-функцияга асосланадиган рақамли имзо схемаси. Бир мартали имзолар схемасидаги камчиликларни бартараф қилиш учун қўлланилади. Ҳар бир янги хабар учун калит жуфтини генерациялашдан воз кечиш имконини беради.

**Дескриптор**  
**uz** - дескриптор  
**en** - descriptor

Элемент информационной структуры, который описывает форму или содержание данных, например, дескриптор сигнатуры – описатель последовательности данных на диске, можно использовать для проверки данных на диске.

Маълумотларнинг шакли ёки мазмунини тавсифловчи ахборот структураси элементи, масалан, сигнатура дескриптори – дискдаги маълумотлар кетма-кетлигини тавсифловчидан дискдаги маълумотларни текширишда фойдаланиш мумкин.

**Дескриптор безопасности**  
**uz** - хавфсизлик дескриптори  
**en** - security descriptor,  
**SD**

Атрибут объекта, содержащий информацию для системы безопасности. Включает идентификатор безопасности владельца объекта, дискреционный и системный список контроля доступа.

Хавфсизлик тизими учун ахборотга эга

## Д

бўлган объект атрибути. Объект эгасининг хавфсизлик идентификаторини, эркин фойдаланишни назорат қилишнинг дискрецион ва тизимга оид рўйхатларини ўз ичига олади.

**Дешифратор**  
**uz** - дешифратор  
**en** - decoder

Логическая схема, преобразующая поразрядное входное двоичное слово (код, шифр) в единичный сигнал на одном из  $2n$  выходов этой схемы.

Разрядма-разряд қирувчи иккилик сўз (код, шифр)ни схеманинг  $2n$  чиқиш учларининг бирида бирилик сигналга ўзгартирувчи мантиқий схема.

**Дешифратор адреса**  
**uz** - адрес дешифратори  
**en** - address decoder

Преобразователь адреса в управляющие сигналы, направляемые запоминающему устройству.

Адресни хотирловчи қурилмага юборилаётган бошқарувчи сигналларга ўзгартиргич.

**Дешифрование**  
**uz** - дешифрлаш  
**en** - decryption, decipherment

1. 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.*

2. Процесс, противоположный шифрованию и связанный с восстановлением исходного текста из зашифрованного при отсутствии ключа шифрования.

1. Шифрланган матндан тегишли дастлабки маълумотларни олиш жараёни.

*Изоҳ: Шифрланган матн такроран шифрланishi мумкин, бунда биринчи дешифрлашда дастлабки очиқ матн тикланмайди.*

2. Шифрлашга қарама-қарши ва шифр-

## Д

лаш калити мавжуд бўлмаганда, шифрланган матндан дастлабки матнни тиклаш билан боғлиқ жараён.

### **Деятельность в сфере программного обеспечения незаконная**

**uz** - дастурий таъминот соҳасидаги ноқонуний фаолият  
**en** - software piracy

Непредусмотренная документами деятельность лиц, заключающаяся в копировании и распространении программного обеспечения без соответствующей лицензии.

### **Директория**

**uz** - директория  
**en** - directory

Список всех файлов, размещаемых на диске с указанием имени и местонахождения.

### **Диск основной**

**uz** - асосий диск  
**en** - key disk

Дискда номи ва жойлашган ўрни кўрсатиб жойлаштириладиган барча файллар рўйхати.

Диск, который необходим для запуска программного продукта на выполнение по частям. Такой диск дает гарантию, что программный продукт адекватен законному оригиналу и не является копией.

Дастурий маҳсулотни қисмларга бўлиб ажаришда ишга тушириш учун зарур диск. Бундай диск дастурий маҳсулот қонуний оригинал билан бир хиллигига, унинг нусхаси эмаслигига кафолат беради.

### **Диспетчер доступа**

**uz** - фойдалана олиш диспетчери  
**en** - reference monitor

Защищенная от внешних воздействий совокупность программных и аппаратных средств контроля доступа субъектов к информационным ресурсам в соответствии с установленными правилами.

Белгиланган қоидаларга мувофиқ, субъектларнинг ахборот ресурсларидан фойдалана олишини назорат қилишнинг



## Д

ташки таъсирлардан муҳофазаланган дастурий ва аппарат воситаларининг жами.

### **Доверие к информации**

**uz** - ахборотга бўлган ишонч

**en** - assurance to information

Отсутствие в информации подмены (не-санкционированной модификации ее элементов при сохранении целостности).

Ахборотда алмаштиришларнинг (яхлитлик сақланиши учун ахборот элементларини рухсатсиз ўзгартиришнинг) бўлмаслиги.

### **Доказательство**

**uz** - далил

**en** - evidence

Информация, которая сама по себе или при использовании вместе с другой информацией может применяться для разрешения спора.

*Примечания:*

1. Конкретными формами доказательств являются цифровые подписи, защитные оболочки и маркеры безопасности.

2. Цифровые подписи используются вместе с методами открытых ключей, тогда как защитные оболочки и маркеры безопасности применяются вместе с методами секретных ключей.

Ўзича ёки бошқа ахборот билан бирга фойдаланилганда, баҳсни ҳал қилиш учун қўлланилиши мумкин бўлган ахборот.

*Изоҳлар:*

1. Рақамли имзолар, ҳимоя қобиклари ва хавфсизлик маркерлари далилнинг аниқ кўринишлари ҳисобланади.

2. Рақамли имзолардан очиқ калитлар методлари билан бирга фойдаланилади, ҳимоя қобиклари ва хавфсизлик маркерлари эса махфий калитлар методлари билан бирга қўлланилади.

### **Домен**

**uz** - домен

**en** - domain

1. Уникальный контекст (например, параметры контроля доступа) исполнения программы, множество объектов, к кото-

## Д

рым субъект может иметь доступ. Имеет иерархическую структуру.

2. Группа компьютеров, которая использует общий список учетных записей, хранящийся на контроллерах домена.

1. Субъект фойдалана олиши мумкин бўлган кўплаб объектларнинг дастурларини бажаришнинг ноёб контексти (масалан, эркин фойдаланишни назорат қилиш параметрлари). Иерархик структурага эга.

2. Домен контроллерларида сақланадиган ҳисобга олинадиган ёзувларнинг умумий рўйхатидан фойдаланадиган компьютерлар гуруҳи.

### Домен безопасности

**uz** - хавфсизлик домени

**en** - security domain

Ограниченная группа объектов и субъектов безопасности, к которым применяется одна политика безопасности со стороны одного и того же администратора безопасности.

Айнан бир хавфсизлик маъмури томонидан битта хавфсизлик сиёсати қўлланиладиган хавфсизлик объектлари ва субъектларининг чекланган гуруҳи.

### Допуск

**uz** - рухсат бериш

**en** - clearance

Разрешение, выданное лицу на право доступа к данным или информации заданного или более низкого уровня безопасности.

Шахсга даражаси белгиланган ёки бирмунча паст бўлган хавфсизлик маълумотлари ёки ахборотдан фойдалана олиш ҳуқуқига берилган рухсат.

### Дорожка дополнительная

**uz** - қўшимча йўлка

**en** - extra track

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

## Д

Нусха кўчиришдан ҳимоя қилиш методи-нинг қисми, бунда дискка стандарт мик-дордаги йўлкалар устидан яна битта йўлка ёзилади.

**Дорожка смещённая**  
**uz** - силжиган йўлка  
**en** - offset track

Часть метода защиты от копирования, когда дорожка на диск записывается в нестандартную позицию.

**Дорожка спираль-ная**  
**uz** - спираль йўлка  
**en** - spiral track

Нусха кўчиришдан ҳимоя қилиш методи-нинг қисми, бунда дискдаги йўлка нос-тандарт позицияга ёзилади.

Часть метода защиты от копирования, когда на диск записывается дорожка спиральной формы.

**Дорожка широкая**  
**uz** - кенг йўлка  
**en** - wide track

Нусха кўчиришдан ҳимоя қилиш методи-нинг қисми, бунда дискка спираль шак-лидаги йўлка ёзилади.

Часть метода защиты от копирования, ко-гда в две или более смежные дорожки на диске записаны одни и те же данные.

**Доска сообщений**  
**uz** - хабарлар тахтаси  
**en** - bulletin board

Нусха кўчиришдан ҳимоя қилиш методи-нинг қисми, бунда дискдаги икки ёки ун-дан ортиқ ёнма-ён йўлкага айнан бир хил маълумотлар ёзилади.

Часть вычислительной системы, реали-зующая функции электронной почты по рассылке и сбору сообщений.

**Достоверность**  
**uz** - ишончлилиқ  
**en** - validity, adequacy

Ҳисоблаш тизимининг хабарларни тарқа-тиш ва йиғиш бўйича электрон почта функциясини амалга оширувчи қисми.

1. Идентичность объекта защиты заяв-ленному.
2. Степень соответствия данных, храни-

## Д

мых в памяти ЭВМ или документах, реальному состоянию отображаемых ими объектов предметной области.

1. Муҳофаза объектнинг мавжуд объектга ўхшашлиги.

2. Электрон ҳисоблаш машиналарининг хотирасида ёки ҳужжатларда сақланадиган маълумотларнинг, улар акс этирадиган предмет соҳанинг ҳақиқий ҳолатига мос келиш даражаси.

### **Достоверность информации**

**uz** - ахборотнинг ишончлилиги  
**en** - information integrity

Оценка вероятности отсутствия ошибок в информации.

Ахборотда хатонинг бўлмаслик эҳтимоллигини баҳолаш.

### **Достоверность обработки информации**

**uz** - ахборотни қайта ишлаш ишончлилиги  
**en** - data processing validity

Функция вероятности ошибки, т.е. события, состоящего в том, что информация в системе не совпадает в пределах заданной точности с некоторым ее истинным значением.

Хато эҳтимоллиги функцияси, яъни тизимдаги ахборот берилган аниқлик чега-расида ахборотнинг баъзи ҳақиқий қиймати билан мос тушмаслигида ифодаланадиган ҳодисалар.

### **Достоверность передачи информации**

**uz** - ахборотни узатишнинг ишончлилиги  
**en** - data transmission validity

Соответствие принятой информации переданной.

Қабул қилинган ахборотнинг узатилган ахборотга мос келиши.

### **Достоверность функциональная**

**uz** - функционал

Свойство соответствия безопасности некоторым критериям, определяемым, например, политикой безопасности.

## Д

ишончилиги  
en - functional  
reliability

### Доступ

uz - фойдалана олиш  
en - access

Хавфсизликнинг баъзи критерийларга, масалан, хавфсизлик сиёсати билан белгиланадиган критерийларга мос келиш хусусияти.

1. Специальный тип взаимодействия между субъектом и объектом, в результате которого создается поток информации от одного к другому.
2. Запрос процесса на открытие объекта для последующего выполнения над ним операций определенного типа.

1. Субъект ва объект ўртасидаги ўзаро ҳамкорликнинг махсус тури, унинг натижасида уларнинг биридан иккинчисига ўтувчи ахборот оқими пайдо бўлади.
2. Маълум турдаги операцияларни кейинчалик бажариш учун объектнинг очилишига сўров жараёни.

### Доступ алгоритмический

uz - алгоритмик фойдалана олиш  
en - algorithmic access

Доступ, основанный на вычислении адреса по некоторому алгоритму.

Қандайдир алгоритм бўйича адресни ҳисоблашга асосланган фойдалана олиш.

### Доступ групповой (коллективный)

uz - гуруҳ (жамоа) бўлиб фойдалана олиш  
en - shared access

Совместное использование вычислительной системы двумя или более пользователями в пакетном или интерактивном режимах.

Икки ёки ундан кўп фойдаланувчининг пакетли ёки интерактив режимда ҳисоблаш тизимидан биргаликда фойдаланиши.

### Доступ дискреционный (избирательный)

uz - дискрецион (танлаб) фойдалана олиш

Метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит. Управление является избира-

## Д

**en** - discretionary  
(selective)  
access

тельным в том смысле, что субъект с определенными правами может осуществлять передачу прав любому объекту независимо от установленных ограничений (доступ может быть осуществлен и не напрямую).

Фойдаланувчи, жараён ва/ёки у тегишли бўлган гуруҳни идентификация қилиш ва танишга асосланган, объектлардан тизим субъектларининг эркин фойдаланишини бошқариш методи. Маълум ҳуқуқларга эга субъект исталган объектга, белгиланган чеклашлардан қатъи назар, ҳуқуқларни беришни амалга ошириши мумкин бўлганда, бошқарув сайланма ҳисобланади (фойдалана олиш – бевосита бўлмаган тарзда ҳам амалга оширилиши мумкин).

**Доступ к информации**

**uz** - ахборотдан фойдалана олиш  
**en** - access to  
information

1. Ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.  
2. Процесс ознакомления с информацией, ее документирование, модификация или уничтожение, осуществляемые с использованием штатных технических средств.

1. Ахборот билан танишиш, уни қайта ишлаш, хусусан, ахборотдан нусха кўчириш, ўзгартириш ёки йўқ қилиш.

2. Ахборот билан танишиш жараёни, уни штат техник воситалардан фойдаланиб, ҳужжатлаштириш, ўзгартириш ёки йўқ қилиш.

**Доступ к информации несанкционированный**

**uz** - ахборотдан руҳсат этилмаган тарзда фойдалана олиш

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

## Д

**en** - unauthorized access to information

Ҳисоблаш техникаси воситалари ёки автоматлаштирилган тизим тақдим этадиган штат воситаларидан фойдаланган ҳолда эркин фойдаланишни чеклаш қоидаларини бузувчи ахборотдан фойдалана олиш.

**Доступ к информации санкционированный**

**uz** - ахборотдан рухсат этилган тарзда фойдалана олиш  
**en** - authorized access to information

Доступ к информации, не нарушающий установленные правила разграничения доступа.

**Доступ к информационному ресурсу**

**uz** - ахборот ресурси-дан фойдалана олиш  
**en** - access to information resource

Получение субъектом доступа возможности манипулировать (использовать, управлять, изменять характеристики и т.п.) данным информационным ресурсом.

Субъектнинг маълум бир ахборот ресурси билан манипуляция қилиш (фойдаланиш, бошқариш, характеристикаларини ўзгартириш ва ш.к.) имкониятига эга бўлиши.

**Доступ к сведениям, составляющим государственную секретность**

**uz** - давлат сири бўлган маълумотлардан фойдалана олиш  
**en** - access to state secret information

Санкционированное полномочным должностным лицом фактическое ознакомление конкретного лица со сведениями, составляющими государственную секретность.

Ваколатли мансабдор шахс томонидан рухсат этилган тарзда, муайян шахсни давлат сири бўлган маълумотлар билан таништириш.

**Доступ к секретной информации несанкционированный**

**uz** - махфий ахборот-

Получение секретных сведений лицами, не имеющими к ним права доступа.

Махфий маълумотлардан фойдалана

## Д

дан рухсат этилмаган  
тарзда фойдалана олиш  
en - unauthorized access  
to secret information

**Доступ к файлу**  
uz - файлга кира  
олиш  
en - file access

**Доступ мандатный**  
uz - мандатли фойда-  
лана олиш  
en - mandatory access

олиш хукукига эга бўлмаган шахслар то-  
монидан махфий маълумотларнинг оли-  
ниши.

Просмотр, модификация, замена или  
удаление файла, а также просмотр и ма-  
нипулирование его атрибутами.

Файлни кўриб чиқиш, ўзгартириш, ал-  
маштириш ёки ўчириб ташлаш, шунинг-  
дек, унинг атрибуларини кўриб чиқиш  
ва уларни манипуляция қилиш.

Способ управления доступом к объектам,  
основанный на степени секретности или  
критичности информации (представленной  
специальными метками), содержащейся в  
объекте и формальной проверке полномо-  
чий и прав субъекта при доступе к инфор-  
мации данного уровня критичности.

Мандатное управление доступом подра-  
зумевает, что:

- все субъекты и объекты системы одно-  
значно идентифицированы;
- каждому объекту системы присвоена  
метка критичности, определяющая цен-  
ность содержащейся в нем информации;
- каждому объекту системы присвоен  
базовый уровень безопасности (уровень  
прозрачности), определяющий максималь-  
ное значение метки критичности объектов,  
к которым субъект имеет доступ.

Объектлардан фойдалана олишни бошқа-  
риш усули. Объектда мавжуд бўлган ах-  
боротнинг махфийлик ёки критиклик да-  
ражасига, маълум бир критиклик даража-  
сидаги ахборотдан фойдалана олишда  
субъектнинг ваколатлари ва ҳуқуқларини



## Д

расман текширишга асосланган.

Фойдалана олишни мандатли бошқариш:

– тизимнинг барча субъектлари ва объектлари бир хил идентификация қилинганлигини;

– тизимнинг ҳар бир объектига, ундаги ахборотнинг қийматини белгиловчи критиклик белгиси берилганлигини;

– тизимнинг ҳар бир объектига субъект фойдалана олиши мумкин бўлган объектлар критиклик белгисининг максимал қийматини ўрнатовчи базавий хавфсизлик даражаси берилишини назарда тутати.

**Доступ мошеннический**

**uz** - фирибгарлик  
оркали фойдалана  
олиш

**en** - fraud access

Несанкционированное использование услуг сотовой связи путем перепрограммирования серийных номеров сотовых аппаратов.

Сотали аппаратларнинг серия рақамларини қайта дастурлаш йўли билан сотали алоқа хизматларидан рухсат этилмаган тарзда фойдаланиш.

**Доступ на запись**

**uz** - ёзиб олишга рухсат

**en** - write access

Право на доступ, при получении которого разрешается записывать данные.

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

Маълумотларни ёзиб олиш учун рухсат берадиган фойдалана олиш ҳуқуқи.

*Изоҳ: Ёзиб олишга рухсат маълумотларни тўлдириш, ўзгартириш, ўчириш ёки яратишга рухсат ҳисобланади.*

**Доступ на чтение**

**uz** - ўқиш учун рухсат

**en** - read access

Право на доступ, при получении которого разрешается читать данные.

Маълумотларни ўқиш учун рухсат берадиган фойдалана олиш ҳуқуқи.

**Доступ неавторизо-**

Преднамеренное обращение пользователя

## Д

### ванный

**uz** - муаллифлаштирилмаган фойдалана олиш

**en** - illegal access

к данным, доступ к которым ему не разрешен, с целью их чтения, модификации или разрушения.

Фойдаланувчининг, ўқиш, ўзгартириш ёки бузиш мақсадида, унга эркин фойдаланиш рухсат этилмаган маълумотларга атайлаб муурожаат қилиши.

### Доступ несанкционированный

**uz** -рухсат этилмаган тарзда фойдалана олиш

**en** - unauthorized access

1. Доступ субъекта к объекту или информации в нарушение установленных в системе правил разграничения доступа.
2. Доступ к сетевым ресурсам, осуществляемый в обход установленной защиты.
3. Нарушение регламентированного доступа к объекту защиты.

1. Субъектнинг объектдан ёки ахборотдан, тизимда белгиланган фойдаланишни чегаралаш қоидаларини бузган ҳолда, фойдалана олиши.

2. Тармоқ ресурсларидан ўрнатилган муҳофазани четлаб ўтиб фойдалана олиш.

3. Муҳофаза объектдан регламентланган тарзда фойдалана олишнинг бузилиши.

### Доступ при отказе

**uz** - ишламай

қолишда

фойдалана олиш

**en** - failure access

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

Ускуна ёки дастурий таъминотнинг бузилиши натижасида йўл қўйилиши мумкин бўлган маълумотларни қайта ишлаш тизимидаги маълумотлардан рухсат этилмаган тарзда ва тасодифий фойдалана олиш.

### Доступность

**uz** - фойдалана олиш-

1. Свойство данных или ресурсов быть доступными и пригодными к использова-

## Д

лик  
en - availability

нию по запросу уполномоченного логического объекта.

2. Возможность за приемлемое время получить от информационной системы требуемую информационную услугу.

1. Маълумотлар ёки ресурсларнинг, ваколатли мантикий объектнинг сўровига кўра, фойдалана олиш мумкин бўлган ва фойдаланишга яроқлилик хусусияти.

2. Мақбул вақт ичида ахборот тизимидан талаб қилинадиган ахборот хизматини олиш мумкинлиги.

**Доступность информации**  
uz - ахборотдан фойдалана олишлик  
en - information availability

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

Ахборот ва унинг ташувчисининг ҳолати, унда фойдаланувчилар томонидан улар учун мўлжалланган ахборотнинг ҳеч қандай қаршиликсиз ва ўз вақтида олиниши таъминланади.

**Доступность системы**  
uz - тизимдан фойдалана олишлик  
en - system availability

Свойство системы, в которой циркулирует информация (средств и технологии ее обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к информации, имеющих на это надлежащие полномочия.

Тегишли ваколатлари бўлган субъектларнинг ахборотдан ўз вақтида ҳеч қандай тўсиқларсиз фойдалана олишини таъминлаш қобилиятини тавсифловчи ахборот (уни қайта ишлаш воситалари ва технологиялари) айланадиган (тарқаладиган) тизимнинг хусусияти.

## Д

**Драйвер устройства**  
uz - курилма драйвери  
en - device driver

Программа, написанная специально для данного устройства с целью обеспечить функцию управления этого устройства со стороны операционной системы.

Операцион тизим томонидан шу курилмани бошқариш функциясини таъминлаш мақсадида мазкур курилма учун махсус ёзилган дастур.

**Дыра**  
uz - тешик  
en - loophole

В вычислительной технике – недоработки, ошибки в программном обеспечении или аппаратуре, позволяющие обойти процессы управления доступом.

Ҳисоблаш техникасида – дастурий таъминот ёки аппаратурадаги фойдалана олишни бошқариш жараёнларини четлаб ўтиш имконини берувчи хатолар, камчиликлар.

## Ж

**Жетон идентификатора личности**  
uz - шахс идентификатори жетони  
en - intelligent token

Миниатюрное устройство, содержащее микропроцессор и память, которое может использоваться в качестве удостоверения личности при работе на терминале.

Таркибида микропроцессор ва хотира бўлган, терминалда ишлаш пайтида шахсий гувоҳнома сифатида фойдаланилиши мумкин бўлган ихчам курилма.

**Живучесть**  
uz - яшовчанлик  
en - viability

Свойство системы (сети) оставаться работоспособной в условиях внешних воздействий.

Тизим (тармок)нинг ташқи таъсирлар шароитида ишга лаёқатли ҳолатини сақлаб қолиш хусусияти.

**Журнал**  
uz - журнал

1. В вычислительной технике – набор данных (файл), используемый операци-

## Ж

en - journal, log

онной или иной системой для сбора и учета статистической информации, различных сообщений и других данных.

2. Файл регистрации или список транзакций, происходящих в компьютере или сети, служащий вспомогательным средством для восстановления событий или данных при потере или порче.

1. Ҳисоблаш техникасида – операцион ёки бошқа тизим томонидан статистик ахборотни, турли хабарлар ва бошқа маълумотларни тўплаш ҳамда ҳисобга олиш учун фойдаланиладиган маълумотлар тўплами (файл).

2. Йўқолганда ёки бузилганда воқеалар ёки маълумотларни тиклаш учун ёрдамчи восита бўлиб хизмат қиладиган, компьютер ёки тармоқда юз берадиган транзакциялар рўйхати ёки қайд этиш файли.

**Журнал аудита**

uz - аудит журнали

en - audit trail

1. Данные, собираемые для последующего использования при проведении аудита безопасности.

2. Совокупность записей о выполняемых в системе транзакциях, документирующая процесс обработки информации в системе и позволяющая определить источники возникновения транзакций в системе и последовательность их выполнения системой.

1. Хавфсизлик аудитини ўтказишда фойдаланиш мақсадида тўпланадиган маълумотлар.

2. Тизимда амалга ошириладиган транзакциялар тўғрисидаги ёзувлар йиғиндиси. Тизимда ахборотнинг қайта ишланиш жараёнини ҳужжатлаштиради, транзакцияларнинг юзага келиш манбаларини ва ти-

## Ж

зим томонидан уларнинг бажарилиш кетма-кетлигини аниқлаш имконини беради.

### **Журнал восстановления**

**uz** - тиклаш журнали  
**en** - recovery log

Журнал, обеспечивающий возможность восстановления базы данных или файла. Содержит информацию о всех изменениях в базе данных (файле) с того момента, когда было установлено, что данные достоверны и была сделана последняя резервная копия.

Маълумотлар базаси ёки файлни тиклаш имкониятини таъминловчи журнал. Маълумотлар ишончли эканлиги ва охири резерв нусха қилинганлиги белгиланган вақтдан бошлаб, маълумотлар базасидаги (файлдаги) барча ўзгартиришлар тўғрисидаги ахборотни ичига олади.

### **Журнал ошибок**

**uz** - хатолар журнали  
**en** - error log

Файл, в который система записывает информацию о сбоях.

Тизим, тўхтаб қолишлар тўғрисидаги ахборотни ёзадиган файл.

### **Журнализация**

**uz** - журналлаштириш  
**en** - journalizing

Процесс записи в системный журнал информации о сообщениях, запросах, выполнявшихся программах, использованных наборах данных и других сведений.

Тизим журналига хабарлар, сўровлар, бажариладиган дастурлар, фойдаланилган маълумотлар тўплами тўғрисидаги ахборотни ва бошқа маълумотларни ёзиш жараёни.

## З

### **Завершение аварийное**

**uz** - авариявий тугаланиш

1. Незапланированное прерывание обработки данных.
2. Преждевременное завершение работы программы из-за программной или аппарат-

**en** - abnormal end,  
abend

ной ошибки, обнаруженной операционной системой. Сопровождается сообщением об ошибке (в отличие от зависаний).

1. Маълумотларни қайта ишлашнинг режалаштирилмаган тарзда тўхтатилиши.

2. Операцион тизим аниқлаган дастур ёки аппарат билан боғлиқ хато тужайли дастур ишининг муддатидан аввал тугалланиши. Хато тўғрисидаги хабар остида боради (осилиб қолишлардан фарқли равишда).

**Зависание програм-  
мы**

**uz** - дастурнинг осилиб қолиши

**en** - program hang-up

Непредусмотренный останов программы, обусловленный, например, такими причинами, как попытка обращения к устройству, не подключенному к процессору.

Дастур ишининг, масалан, процессорга уланмаган қурилмага мурожаат қилишга уриниш каби сабабга боғлиқ равишда кўзда тутилмаган тўхтаб қолиши.

**Зависание системы**

**uz** - тизимнинг осилиб қолиши

**en** - system quiescing

Остановка («замораживание») мультипрограммной системы путем подавления ввода новых заданий.

Мультидастурли тизимни янги топшириқлар киритилишини бостириш йўли билан тўхтатиш («музлатиб қўйиш»).

**Загрузка по линиям телекоммуникаций**

**uz** - телекоммуникациялар линиялари бўйлаб юклаш

**en** - download

Пересылка программного обеспечения по линии телекоммуникаций от одной компьютерной системы к другой, например, от сервера к персональному компьютеру.

Телекоммуникациялар линияси бўйлаб дастурий таъминотни бир компьютер тизимидан бошқасига, масалан, сервердан шахсий компьютерга ўтказиш.

**Загрязнение**

Введение данных с одним грифом сек-

**uz** - ифлосланиш  
**en** - contamination

ретности или категорией безопасности в данные с более низким грифом секретности или другой категорией безопасности.

**Задание по безопасности**

**uz** - хавфсизлик  
бўйича топширик  
**en** - security target

Совокупность требований безопасности и спецификаций, предназначенных для использования в качестве основы для оценки конкретного объекта оценки.

Муайян баҳолаш объектини баҳолаш учун асос сифатида фойдаланишга мўлжалланган, хавфсизлик талаблари ва спецификациялар йиғиндиси.

**Задача контрольная**

**uz** - назорат  
топшириғи  
**en** - check problem

Задача с известным решением, используемая для определения правильности работы функционального модуля.

Функционал модуль иши тўғрилигини аниқлаш учун фойдаланиладиган, ечими маълум топширик.

**Задача перехвата**

**uz** - қўлга киритиш  
масаласи  
**en** - interception  
problem

Задача получения информации, которая решается на основе обработки перехваченных побочных электромагнитных излучений и наводок.

Ахборотни олиш масаласи, тутиб олинган номақбул электромагнит нурланишлар ва таъсирларни қайта ишлаш асосида ҳал этилади.

**Замещение**

**uz** - ўрнини босиш  
**en** - replay (attack)

Вид атаки в криптосистеме или системе аутентификации, при которой сообщение запоминается и передается вновь позднее,



замещая или повторяя первоначальное сообщение.

Криптотизим ёки аутентификация қилиш тизимидаги хужум тури. Бунда хабар ёдда сакланади ва бошланғич хабарнинг ўрнини босган ёки такрорлаган ҳолда, кейинрок яна узатилади.

**Замок защиты (секретности)**

**uz** - муҳофаза (махфийлик) кулфи

**en** - privacy lock, protection lock

Программный механизм проверки паролей при обращении к базе данных или ее фрагментам (файлам, областям), обеспечивающий ограничение доступа к записям.

Маълумотлар базасига ёки унинг фрагментларига (файлларга, соҳаларга) мурожаат қилингандаги паролларни текширишнинг дастурий механизми. Ёзувлардан фойдаланишни чеклайди.

**Замок памяти**

**uz** - хотира кулфи

**en** - memory lock

Код в дескрипторе сегмента или страницы виртуальной памяти, используемый системой защиты памяти для ограничения доступа. При этом к сегменту могут обращаться только процессы, имеющие в своем дескрипторе соответствующий ключ.

Хотиранинг муҳофаза тизими томонидан фойдаланишни чеклаш учун ишлатиладиган, сегмент дескрипторидаги код ёки виртуал хотира саҳифаси коди. Бунда сегментга ўз дескрипторида тегишли калитга эга бўлган жараёнларгина мурожаат қила олади.

**Замысел защиты информации**

**uz** - ахборотни муҳофаза қилиш

гояси

Основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность мероприятий, необходимых для достижения цели защиты информации на объекте.

**en** - information security plan

Объектда ахборотни муҳофаза қилиш мақсадларига эришиш учун зарур бўлган тадбирларнинг таркиби, мазмуни, ўзаро алоқадорлиги ва кетма-кетлигини очиб берувчи асосий фикр (ғоя).

**Запись контрольная**  
**uz** - назорат ёзуви  
**en** - control record

Запись, которая содержит контрольные суммы, вычисленные путем суммирования значений из других записей файла. Контрольные суммы могут нести дополнительную информацию или использоваться только для проверки правильности данных.

Файлдаги бошқа ёзувлар қийматларини жамлаш йўли билан ҳисобланган назорат суммаларини ўз ичига олувчи ёзув. Назорат суммалари қўшимча ахборотга эга бўлиши ёки фақат маълумотларнинг тўғрилигини текшириш учун қўлланилиши мумкин.

**Запись учетная**  
**uz** - ҳисобга олиш ёзуви  
**en** - account

Информация, идентифицирующая субъект системы безопасности. Указателем на учетную запись является ее идентификатор безопасности. Различают учетные записи пользователей, групп, компьютеров и доменов.

Хавфсизлик тизими субъектини идентификация қилувчи ахборот. Ҳисобга олиш ёзувининг кўрсаткичи бўлиб, унинг хавфсизлик идентификатори ҳисобланади. Фойдаланувчилар, гуруҳлар, компьютерлар ва доменларнинг ҳисобга олиш ёзувлари ажратилади.

**Заполнение страницы**  
**uz** - саҳифани тўлдириш  
**en** - page padding

Способ записи в блок данных последней не полностью заполненной страницы незначашей информации.

Маълумотлар блокига аҳамиятли бўлма-

ган ахборотнинг охирги, тўлик тўлдирилмаган саҳифасини ёзиш усули.

**Заполнение трафика**

**uz** - трафикни

тўлдириш

**en** - traffic padding

Контрмера, при использовании которой средства передачи генерируют ложные данные, чтобы затруднить выполнение анализа трафика или его дешифрование.

Қарши чора, ундан фойдаланишда уза-тиш воситалари трафикни таҳлил қилиш ёки унинг қайта шифрланишини қийинлаштириш мақсадида ёлгон маълумотларни генерациялайди.

**Запрос/ответ**

**uz** - сўров/жавоб

**en** - challenge/response

Метод аутентификации, при котором одна сторона посылает зашифрованный запрос, а вторая выдает ответ с помощью одного и того же алгоритма аутентификации.

Аутентификация методи, унга кўра, бир томон шифрланган сўров жўнатади, иккинчи томон эса, айнан битта аутентификация алгоритми ёрдамида жавоб беради.

**Засекречивание сведений и их носителей**

**uz** - маълумотлар ва уларнинг ташувчиларини махфийлаштириш

**en** - classification of information and its bearers as secret

Введение в предусмотренном законодательством порядке для сведений, составляющих государственные секреты, ограничений на их распространение и на доступ к их носителям.

Қонунда кўзда тутилган тартибда, давлат сири ҳисобланадиган маълумотлар учун, уларни тарқатиш ва ташувчилардан фойдаланиш юзасидан чеклашлар киритиш.

**Захватчики паролей**

**uz** - паролларни эгаллаб олувчилар

**en** - password hook

Программы, ворующие пароли путем обманных воздействий на операционную систему.

Операцион тизимга алдамчи таъсирлар

кўрсатиш орқали паролларни ўғирловчи дастурлар.

### **Защитывание**

**uz** - цикллаш

**en** - cycling

1. Автоматическое объединение конца одной строки с началом другой, когда это касается дисплея или принтера.

2. Автоматическое объединение конечной области ПЗУ с начальной.

1. Бир сатр охирини бошқа сатр боши билан, бу дисплей ёки принтерга тааллуқли бўлганда, автоматик бирлаштириш.

2. Доимий хотирловчи курилманинг охирги соҳасини бошланғич соҳа билан автоматик бирлаштириш.

### **Зашифрование**

**uz** - шифрлаш

**en** - coding

Процесс применения обратимого преобразования шифра к открытому тексту. Результатом зашифрования является шифротекст.

Шифрни очик матнга ўзгартиришни кўллаш жараёни. Шифр матн шифрлаш натижаси ҳисобланади.

### **Защита**

**uz** - муҳофаза қилиш

**en** - security

Юридические, организационные и технические, в том числе программные, меры предотвращения несанкционированного доступа к аппаратуре, программам и данным.

Аппаратура, дастурлар ва маълумотлардан рухсат этилмаган тарзда фойдаланишнинг олдини олиш бўйича юридик, ташкилий, техник, шу жумладан, дастурий чора-тадбирлар.

### **Защита аппаратная**

**uz** - аппарат воситасида муҳофаза қилиш

Использование аппаратных средств, например, регистров границ или замков и ключей для защиты данных в ЭВМ.

en - hardware security

Аппарат воситалардан, масалан, чегаравий регистрларидан ёки кулфлар ва калитлардан ЭХМдаги маълумотларни муҳофаза қилиш учун фойдаланиш.

**Защита  
вычислительной  
сети**

uz - ҳисоблаш тармоғини муҳофаза қилиш

en - network security

Исключение несанкционированного доступа пользователей к элементам и ресурсам сети путем использования аппаратных, программных и криптографических методов и средств защиты, а также организационных мероприятий.

Аппарат, дастурий ва криптографик муҳофаза қилиш методлари ҳамда воситаларидан, шунингдек, ташкилий тадбирлардан фойдаланиш йўли билан фойдаланувчиларнинг тармоқ элементлари ҳамда ресурсларидан рухсат этилмаган тарзда фойдалана олишларига йўл қўймаслик.

**Защита данных**

uz - маълумотларни муҳофаза қилиш

en - data protection

1. Реализация административных, технических или физических мер для предотвращения несанкционированного доступа к данным.

2. Меры, предпринимаемые для сохранения данных от нежелательных последствий и действий, которые неумышленно или преднамеренно ведут к модификации, раскрытию или разрушению данных.

1. Маълумотлардан рухсат этилмаган тарзда фойдалана олишнинг олдини олиш учун маъмурий, техник ёки жисмоний чора-тадбирларни амалга ошириш.

2. Маълумотларни қасдан ёки қасдан бўлмаган тарзда ўзгартирилишига, фож бўлишига ёки бузилишига олиб келадиган номақбул оқибатлардан ва ҳаракат-

лардан сақлаш учун қўлланиладиган чора-тадбирлар.

**Защита информации (данных)**

**uz** - ахборотни (маълумотларни) муҳофаза қилиш  
**en** - information (data) security

1. Комплекс правовых, организационных и технических (программно-аппаратных) мероприятий, направленных на предотвращение или затруднение нанесения ущерба интересам собственника информации (данных).

2. Меры по предотвращению угроз информационной безопасности и устранению их последствий.

3. Деятельность, направленная на предотвращение утечки защищаемой информации, от несанкционированных и непреднамеренных воздействий на защищаемую информацию.

1. Ахборот (маълумот) эгаси манфаатларига зарар келтирилишининг олдини олиш ёки қийинлаштиришга қаратилган ҳуқуқий, ташкилий ва техник (аппаратдастурий) тадбирлар комплекси.

2. Ахборот хавфсизлигига бўладиган таҳдидларнинг олдини олиш ва уларнинг оқибатларини бартараф қилиш бўйича қўриладиган чора-тадбирлар.

3. Муҳофаза қилинадиган ахборот чиқиб кетиши (йўқолиши) муҳофаза қилинадиган ахборотга рухсат этилмаган ва кўзда тутилмаган таъсир(лар)ни бартараф этишга қаратилган фаолият.

**Защита информации организационная**

**uz** - ахборотни ташкилий жиҳатдан муҳофаза қилиш  
**en** - organizational security of information

Защита информации при ее обработке техническими средствами, осуществляемая путем принятия административных мер.

*Примечание: Административные меры включают выбор места расположения объекта, не подверженного внешним воздействиям, организацию контролируемой (проверяемой) зоны, выполнение правил учета, хранения и обра-*

ния секретных (конфиденциальных) документов на различных носителях и другие меры.

Техник воситалар билан қайта ишлашда ахборотни муҳофаза қилиш, маъмурий чора-тадбирлар кўриш орқали амалга оширилади.

*Изоҳ: Маъмурий чора-тадбирлар ташиқи таъсирга учрамаган объект жойлашадиган ернинг танланишини, назорат қилинадиган (текишириладиган) зонани ташиқил-лаштириши, турли ташувчилардаги махфий (конфиденциал) ҳужжатларни ҳисобга олиб, сақлаш ва улар билан ишлаш қоидаларини ва бошқа чора-тадбирларни ичига олади.*

**Защита информации организационно-техническая**

**uz** - ахборотни ташкилий-техник жиҳатдан муҳофаза қилиш

**en** - organizational and technical security of information

Защита информации, предусматривающая применение руководящих, нормативных и методических документов, лицензирование деятельности в области защиты информации, сертификацию защищенных изделий, технических средств и способов защиты, создание на объектах систем защиты информации и аттестацию этих объектов.

Раҳбарий, норматив ва методик ҳужжатларнинг қўлланилишини, ахборотни муҳофаза қилиш соҳасида фаолиятни лицензиялашни, муҳофазаланган буюмлар, муҳофаза қилишнинг техник воситалари ҳамда усуллари, объектларда ахборотни муҳофаза қилиш тизимлари тузилишини ва бу объектларнинг аттестация қилинишини кўзда тутадиган ахборотни муҳофаза қилиш.

**Защита информации от несанкционированного воздействия**  
**uz** - ахборотни рухсат

Деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение ин-

этилмаган таъсирдан муҳофаза қилиш  
**en** - information security from illegal impact

формации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Ахборотни ўзгартириш юзасидан белгиланган ҳуқуқлар ва ёки қоидалар бузилган ҳолда, ахборотнинг бузиб кўрсатилишига, йўқ қилинишига, ундан фойдалана олишнинг блокиров-қаланишига, шунингдек, ахборот ташувчининг йўқолишига, йўқ қилинишига ёки ишлашида узилиш келиб чиқишига олиб келадиган таъсирнинг олдини олишга қаратилган фаолият.

**Защита информации от несанкционированного доступа**

**uz** - ахборотни рухсат этилмаган тарзда фойдалана олишдан муҳофаза қилиш  
**en** - information security from unauthorized access

Деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных нормативными документами или собственником (владельцем) информации прав или правил доступа к ней.

Манфаатдор субъектнинг, норматив ҳужжатлар ёки ахборот эгаси томонидан белгиланган ҳуқуқлар ёки ахборотдан фойдаланиш қоидаларини бузиб, муҳофаза қилинадиган ахборотни олишига йўл кўймасликка йўналтирилган фаолият.

**Защита информации от разглашения**

**uz** - ахборотни ошкор этилишдан муҳофаза қилиш  
**en** - information security from disclosure

Деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации.

Муҳофаза қилинадиган ахборотнинг бу ахборотдан фойдалана олиш ҳуқуқи



бўлмаган истъёмолчиларга рухсат этилмаган тарзда етказилишининг олдини олишга қаратилган фаолият.

**Защита информации от утечки**

**uz** - ахборотни чиқиб кетишдан муҳофаза қилиш

**en** - information security from leak flow

Деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации.

Ошкор қилиш, рухсат этилмаган тарзда ахборотдан фойдалана олиш ва муҳофаза қилинадиган ахборотни олиш натижасида муҳофаза қилинадиган ахборотнинг назорат қилиб бўлмайдиган равишда тарқалиб кетишининг олдини олишга қаратилган фаолият.

**Защита информации при ее обработке техническими средствами**

**uz** - ахборотни техник воситалар билан қайта ишлашда муҳофаза қилиш

**en** - information security while processing it with technical facilities

Действия, направленные на обеспечение безопасности информации при ее обработке техническими средствами от всех видов угроз и факторов опасности.

*Примечание: При обработке информации техническими средствами различают организационную и техническую защиты.*

Техник воситалар билан қайта ишлашда барча турдаги таҳдидлардан ва хавф омилларидан ахборотнинг хавфсизлигини таъминлашга қаратилган ҳаракат.

*Изоҳ: Ахборотни техник воситалар билан қайта ишлашда ташкилий ва техник жиҳатдан муҳофаза қилиш фарқланади.*

**Защита информации техническая**

**uz** - ахборотни техник муҳофаза қилиш

**en** - technical protection of information

1. Защита информации при ее обработке техническими средствами, осуществляемая с использованием технических средств и способов защиты.

*Примечание: К техническим средствам и способам защиты информации при ее обра-*

ботке техническими средствами в общем случае относятся аппаратные, автономные (инженерные) и программные средства, а также криптографические методы.

2. Деятельность, направленная на обеспечение безопасности информации инженерно-техническими мерами.

1. Ахборотнинг уни техник воситалар билан қайта ишлаш пайтида муҳофаза қилиниши. Муҳофаза қилишнинг техник воситалари ҳамда усулларидан фойдаланиб амалга оширилади.

*Изоҳ:* Ахборотни техник воситалар билан қайта ишлашда, ахборотни муҳофаза қилишнинг техник воситалари ва усулларига умумий ҳолда аппарат, автоном (инженер) ҳамда дастурий воситалар, шунингдек, криптографик методлар қиради.

2. Инженер-техник чора-тадбирлар ёрдамида ахборот хавфсизлигини таъминлашга қаратилган фаолият.

**Защита криптографическая**

**uz** - криптографик муҳофаза қилиш  
**en** - cryptosecurity, cryptographically security

Защита информации (данных) при помощи ее криптографического преобразования.

Ахборот (маълумотлар)ни, уни криптографик қайта ўзгартириш ёрдамида муҳофаза қилиш.

**Защита личной тайны**

**uz** - шахсий сирни муҳофаза қилиш  
**en** - privacy protection

Реализация мер, гарантирующих сохранение личной тайны. К этим мерам относятся защита персональных данных и ограничения на их сбор, обобщение и обработку.

Шахсий сирнинг сақланишини кафолатловчи чора-тадбирларнинг амалга оширилиши. Бу чора-тадбирларга шахсий маълумотларни муҳофаза қилиш ҳамда уларни

тўплаш, умумлаштириш ва қайта ишлани-  
шини чеклашлар қиради.

**Защита накоплени-  
ем**

**uz** - тўплаш билан  
муҳофаза қилиш  
**en** - security by  
generation

Метод восстановления данных, хранящихся  
во внешней памяти, состоящий в том, что  
на дополнительный носитель копируются  
только те файлы, которые были созданы  
позднее определенного срока.

Ташқи хотирада сақланадиган маълумот-  
ларни тиклаш методи. Қўшимча ташувчига  
маълум бир муддатдан кейин яратилган  
файллар копия қилинишида ифодаланади.

**Защита непосредст-  
венная**

**uz** - бевосита  
муҳофаза қилиш  
**en** - physical security

Меры, предусматривающие физическую  
защиту ресурсов от преднамеренных или  
случайных угроз.

Ресурсларнинг қасдан қилинадиган ёки  
тасодифий таҳдидлардан физик муҳофаза  
қилинишини кўзда тутадиган чора-  
тадбирлар.

**Защита объектов**

**uz** - объектларни  
муҳофаза қилиш  
**en** - object protection

Средства защиты объектов (например, фай-  
лов, носителей, сейфов), которые могут  
быть выведены из защищенной области.

Муҳофазаланган соҳадан чиқарилиши  
мумкин бўлган объектларни (масалан,  
файлларни, ташувчиларни, сейфларни)  
муҳофаза қилиш воситалари.

**Защита от записи**

**uz** - ёзувдан муҳофаза  
қилиш  
**en** - write protect

Способ защиты информации на диске,  
закрывающийся в заклеивании метки  
считывания на дискетах 5.25" и задвижки  
метки считывания на дискетах 3.5", что  
предотвращает запись новых данных и  
сохраняет имеющиеся от разрушения.

Дискдаги ахборотни 5.25" дискеталарида  
солиштириб ўқиш белгисини ёпиштириш

ва 3.5" дискеталарида солиштириб ўқиш белгисини суриб, муҳофаза қилиш усули, бу янги маълумотлар ёзиб олишнинг олдини олади ва мавжуд маълумотларни йўқолишдан сақлайди.

### **Защита от копирования**

**uz** - нусха

кўчирилишидан

муҳофаза қилиш

**en** - copy protection

1. Использование специальных методов для обнаружения или предотвращения несанкционированного копирования данных, программного или аппаратно-программного обеспечения.

2. Способ предотвращения копирования информации, записанной на магнитном носителе, например на диске, содержащем программный продукт коммерческого назначения.

1. Маълумотлардан, дастурий ёки дастурий-аппарат таъминотидан рухсат этилмаган тарзда нусха кўчирилишини аниқлаш ёки олдини олиш учун махсус методларнинг қўлланилиши.

2. Магнит ташувчида, масалан, тижорат йўналишидаги дастурий махсулотга эга дискда ёзилган ахборотдан нусха кўчирилишининг олдини олиш усули.

### **Защита от ошибок**

**uz** - хатолардан

муҳофаза қилиш

**en** - error protection

1. Совокупность аппаратных и/или программных средств, предотвращающих или уменьшающих возможность появления ошибок.

2. Средства и способы контроля допустимости значений входных параметров.

1. Хатолар пайдо бўлиш имкониятини бартараф қилувчи ёки камайтирувчи аппарат ва/ёки дастурий воситалар жами.

2. Кириш параметрлари қийматларининг йўл қўйиб бўлишлигини назорат қилиш воситалари ва усуллари.

**Защита от чтения**

**uz** - ўқишдан муҳофаза қилиш  
**en** - read protection

Запрещение обращения к файлу для выполнения операции чтения данных. Разрешается только запись данных.

Маълумотларни ўқиш учун файлга мурожаат қилишнинг таъқиқланиши. Фақат маълумотларни ёзишга рухсат этилади.

**Защита памяти**

**uz** - хотирани муҳофаза қилиш  
**en** - memory protection, storage protection

1. Механизм контроля за доступом к какой-либо области памяти с учетом разрабатываемых обращений.  
 2. Средства и способы предотвращения несанкционированного доступа к некоторым участкам памяти с целью сохранения неизменности записанных данных.

1. Ишлаб чиқилган мурожаатларни ҳисобга олган ҳолда хотиранинг қандайдир қисмига қира олишни механик назорат қилиш .

2. Ёзилган маълумотларнинг доимийлигини сақлаш мақсадида хотиранинг баъзи бир қисмларига рухсат этилмаган тарзда қиришнинг олдини олиш воситалари ҳамда усуллари.

**Защита паролем**

**uz** - пароль билан муҳофаза қилиш  
**en** - password protection

1. Механизм управления доступом к системе, обеспечивающий сохранение целостности программного обеспечения в составе системы или сети.

2. Способ защиты данных, при котором для получения доступа к ним необходимо ввести пароль.

1. Тизимдан фойдалана олишни бошқариш механизми бўлиб, тизим ёки тармок ичида дастурий таъминот яхлитлиги сақланишини таъминлайди.

2. Маълумотларни муҳофаза қилиш усули, бунда маълумотлардан фойдалана олиш учун пароль киритиш зарур.

**Защита поля избирательная**

**uz** - танланган майдон муҳофазаси  
**en** - selective field protection

**Защита прав пользователей**

**uz** - фойдаланувчилар ҳуқуқларини муҳофаза қилиш  
**en** - user rights protection

**Защита предупредительная**

**uz** - огоҳлантирувчи муҳофаза қилиш  
**en** - disincentive protection

**Защита программы**

**uz** - дастурни муҳофаза қилиш  
**en** - software lock (software protection)

Защита специальных полей в пределах передаваемого сообщения.

Узатиладиган хабар доирасида махсус майдонларни муҳофаза қилиш.

Совокупность правил, методов и средств, направленных на обеспечение беспрепятственного и своевременного доступа пользователей к программам и данным и защиту их информации от использования другими лицами.

Фойдаланувчиларнинг дастурлар ва маълумотлардан тўсқинликларсиз ҳамда ўз вақтида фойдалана олишларини таъминлашга ва улардаги ахборотдан бошқа шахслар фойдаланишидан муҳофаза қилишга қаратилган қоидалар, методлар ҳамда воситалар жами.

Организационные меры защиты от копирования, предусматривающие суровый штраф или угрозу штрафа лицу, которое пытается несанкционированно скопировать программу или файл.

Нусха кўчиришдан муҳофаза қилиш бўйича ташкилий чора-тадбирлар. Дастур ёки файлдан рухсат этилмаган тарзда нусха кўчиришга уринадиган шахс жаримага тортилишини ёки жарима тўлаш тахдидини кўзда тутати.

Совокупность условий, предотвращающих запуск программы на выполнение.

Дастурнинг бажарилиши учун ишга тушириб юборилишини бартараф этувчи

шартларнинг жами.

### **Защита системы**

**uz** - тизимни муҳофаза қилиш  
**en** - system protection  
 (system security)

Совокупность мер, предпринимаемых для исключения несанкционированного доступа к программам и данным системы или случайного вмешательства в ее работу.

Дастурлар ва тизим маълумотларидан рухсат этилмаган тарзда фойдалана олишни ёки тизим ишига тасодифий ара-лашишни бартараф қилиш мақсадида кўриладиган чора-тадбирлар жами.

### **Защита файла**

**uz** - файлни муҳофаза қилиш  
**en** - file protection

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

Файлга рухсатсиз кириш, уни ўзгартириш ёки ўчиришнинг олдини олиш мақсадида тегишли маъмурий, техник ёки физик чора-тадбирларни амалга ошириш.

### **Защита физическая**

**uz** - физик муҳофаза  
**en** - physical protection

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.

Телекоммуникация ёки ахборот тизимлари компонентларини ва уларнинг структурасини жинояткорларнинг қасдан қилинадиган ҳаракатлари ёки хизмат кўрсатувчи ходимларнинг масъулиятсизликлари натижасида етказиладиган физик зарардан ҳимоя қилиш учун мўлжалланган механизм ва процедуралар.

**Защита эшелонированная**

**uz** - бирин-кетин  
жойлаштириб  
муҳофаза қилиш  
**en** - defence-in-depth

Концепция системы безопасности, при которой каждая подсистема в сети защищается до максимально возможного уровня.

Хавфсизлик тизими концепцияси, унда тармокдаги ҳар бир кичик тизим мумкин бўлган максимал даражагача муҳофаза қилинади.

**Защищенность**

**uz** - муҳофаза  
қилинганлик  
**en** - security

Способность системы противостоять несанкционированному доступу к защищаемой информации, ее искажению или разрушению.

Тизимнинг, муҳофаза қилинадиган ахборотдан рухсат этилмаган тарзда фойдалана олишга, унинг бузилишига ёки унга зарар етказилишига қарши тура олиш қобилияти.

**Заявитель**

**uz** - талабгор  
**en** - claimant

Объект, который является администратором доступа в целях аутентификации или представляет его. Заявитель выполняет функции, необходимые для осуществления обменов данными аутентификации от имени администратора доступа.

Аутентификация қилиш мақсадида фойдалана олиш маъмури ҳисобланадиган объект. Талабгор фойдалана олиш маъмури номидан аутентификация маълумотлари алмашинувини амалга ошириш учун зарур бўлган вазифаларни бажаради.

**Злоумышленник**

**uz** - жинояткор  
**en** - intruder, malicious  
user

1. Нарушитель, умышленно действующий из корыстных побуждений.
2. Лицо или организация, заинтересованные в получении несанкционированного доступа к информационной системе и ее ресурсам и совершившие преднамерен-



ные действия для их несанкционированного получения и изменения.

3. Лицо, получившее несанкционированный доступ с целью осуществления злонамеренных вызовов.

4. Лицо, осуществляющее осознанные действия по нарушению информационной безопасности объекта защиты.

1. Ғаразли ниятда қасддан ҳаракат қилувчи бузғунчи.

2. Ахборот тизими ва унинг ресурсларидан рухсат этилмаган тарзда фойдаланишдан манфаатдар бўлган ва уларни рухсат этилмаган тарзда олиш, ўзгартириш учун олдиндан ўйлаб ҳаракат қилган шахс ёки ташкилот.

3. Ёмон ниятдаги чақирувларни амалга ошириш мақсадида рухсат этилмаган фойдалана олишга эга бўлган шахс.

4. Муҳофаза объектининг ахборот хавфсизлиги бузилишини англаган ҳолда ҳаракат қилувчи шахс.

#### **Злоупотребление компьютерное**

**uz** - компьютер суистеъмоллиги

**en** - computer abuse

Умышленное или случайное несанкционированное действие, которое влияет на компьютерную безопасность системы обработки данных или нарушает ее.

Маълумотларни қайта ишлаш тизимининг компьютер хавфсизлигига таъсир этадиган ёки уни бузадиган, қасддан ёки тасодифий рухсат берилмаган ҳаракат.

#### **Знак защитный специальный, СЗЗ**

**uz** - махсус муҳофаза белгиси

**en** - special security mark

Сертифицированное и зарегистрированное в установленном порядке изделие, предназначенное для контроля несанкционированного доступа к объектам защиты путем определения подлинности и целостности самого знака или компози-

ции «Специальный защитный сигнал-подложка» по критериям соответствия характерным признакам.

Белгининг ҳақиқийлигини ва яхлитлигини аниқлаш ёки характерли аломатларга мос келишлик мезонлари бўйича, «Махсус муҳофаза белгиси – таглик» композициясини аниқлаш йўли билан муҳофаза қилинадиган объектлардан рухсат этилмаган тарзда фойдалана олишни назорат қилиш учун мўлжалланган, белгиланган тартибда сертификатланган ва рўйхатга олинган буюм.

**Знак соответствия в области защиты информации**

**uz** - ахборотни муҳофаза қилиш соҳасидаги мувофиқлик белгиси  
**en** - compliance mark in the field of information security

Защищенный в установленном порядке знак, применяемый или выданный в соответствии с правилами системы сертификации, указывающий, что обеспечивается необходимая уверенность в том, что данное защищенное изделие, техническое средство или способ защиты информации соответствуют конкретному стандарту или другому нормативному документу.

Сертификатлаш тизими қоидаларига мувофиқ бериладиган ёки қўлланиладиган, берилган муҳофазаланган буюм, техник восита ёки ахборотни муҳофаза қилиш усули муайян стандартга ёки бошқа норматив ҳужжатга мос келишини кўрсатадиган, белгиланган тартибда муҳофазаланган белги.

**Значение атрибута**  
**uz** - атрибут киймати  
**en** - attribute value

Тип атрибута, который обозначает конкретный экземпляр класса информации, например, персональные имена, и является частью атрибута.

Ахборот классининг маълум бир нусха-сини, масалан, шахсий номларни белгилайдиган атрибут тури. Атрибутнинг бир қисми ҳисобланади.

**Значение контрольное криптографическое**

**uz** - криптографик назорат қиймати  
**en** - cryptographic checkvalue

Информация, определяемая в ходе криптографического преобразования блока данных и предназначенная для контроля целостности передаваемой информации.

Маълумотлар блокени криптографик қайта ўзгартиришда аниқланадиган ва узатиладиган ахборотнинг яхлитлигини назорат қилиш учун мўлжалланган ахборот.

**Значение начальной установки**

**uz** - бошланғич ўрнатиш қиймати  
**en** - initialization value

Последовательность символов, используемая для установки генератора ключевого потока в заданное положение.

Қалит оқими генераторини берилган (маълум бир) ҳолатга ўрнатиш учун қўлланиладиган символлар кетма-кетлиги.

**Значение секретное коллективное**

**uz** - жамоавий махфий қиймат  
**en** - shared secret

Ключ системы защиты для криптографических алгоритмов.

Муҳофаза қилиш тизимининг криптографик алгоритмлар учун мўлжалланган қалити.

**Зона**

**uz** - зона  
**en** - protected area

Область, защищенная системой безопасности.

Хавфсизлик тизими билан муҳофаза қилинган соҳа.

**Зона безопасности**

**uz** - хавфсизлик зонаси  
**en** - safety zone

Механизм, определенный в браузере Microsoft Internet Explorer компании Microsoft, позволяющий задавать настройки безопасности для групп Интернет-

серверов. Для каждой из зон возможно использовать различные уровни безопасности, определяющие возможные действия, допустимые для этого сервера (запуск Java-апплетов, управляющих элементов ActiveX, установление защищенного соединения по протоколу SSL и т.п.).

Интернет-серверлар гурухи учун хавфсизлик созланишлари ўрнатилишига имкон берувчи Microsoft компаниясининг Microsoft Internet Explorer браузериди белгиланган механизм. Зоналарнинг ҳар бири учун шу сервер учун йўл қўйилмаган, мумкин бўлган ҳаракатларни белгиловчи хавфсизликнинг турли даражаларини қўллаш мумкин (Java-апплетларини, ActiveX бошқарувчи элементларини ишга тушириш, SSL протоколи бўйича муҳофазаланган уланишни ўрнатиш ва ш.к.).

**Зона контролируемая**

**uz** - назорат

килинадиган зона

**en** - under control zone

Территория вокруг технического средства обработки информации, в пределах которой не допускается несанкционированное пребывание посторонних лиц и транспортных средств.

Ахборотни қайта ишлаш техник воситаси атрофидаги ҳудуд, унинг чегарасида бегона шахсларнинг ва транспорт воситаларининг рухсат этилмаган тарзда бўлишига йўл қўйилмайди.

**Зона опасная 1**

**uz** - 1-хавфли зона

**en** - 1 danger area

Пространство вокруг технического средства обработки информации, в пределах которого на случайных антеннах наводится опасный сигнал выше допустимого нормированного уровня. В зоне 1 запрещается размещение случайных антенн,

### 3

имеющих выход по токопроводящим коммуникациям за пределы контролируемой зоны.

Ахборотни қайта ишлаш техник воситасининг атрофидаги майдон бўлиб, унинг доирасида тасодифий антенналарда йўл қўйиладиган нормаланган даражадан юқори бўлган хавфли сигнал ҳосил қилинади. Биринчи зонада ток ўтказадиган коммуникациялар орқали назорат қилинадиган зонадан ташқарита чиқиши бўлган тасодифий антенналарни жойлаштириш таъқиқланади.

**Зона опасная 2**  
**uz** - 2-хавфли зона  
**en** - 2 danger area

Пространство вокруг технического средства обработки информации, в пределах которого отношение опасный сигнал/помеха для составляющих напряженности электромагнитного поля превышает допустимое нормированное значение.

Ахборотни қайта ишлаш техник воситасининг атрофидаги майдон бўлиб, унинг доирасида электромагнит майдон кучланганлигини ташкил этувчилар учун хавфли сигнал/халақит нисбати йўл қўйиладиган нормаланган қийматдан ошади.

### И

**Идентификатор**  
**uz** - идентификатор  
**en** - identifier, ID

1. Символ или последовательность символов (сигналов) для обозначения ими наименования определенной совокупности сведений.
2. Код или символическое имя, однозначно характеризующее объект и позволяющее выделить его среди множества других объектов. Идентификатор

## И

может указывать на тип сети, протокол, номер порта и др.

3. Средство идентификации доступа, представляющее собой отличительный признак субъекта или объекта доступа. Основным средством идентификации доступа для пользователей является пароль.

1. Маълумотларнинг маълум тўшлами ни номлаш учун қўлланиладиган символ ёки символлар (сигналлар) кетма-кетлиги.

2. Объектни тавсифловчи ва уни бошқа кўплаб объектлар орасида ажратиб кўрсатиш имконини берувчи код ёки рамзий ном. Идентификатор тармоқ типини, протоколинни, порт рақамини ва б.к. кўрсатиши мумкин.

3. Фойдалана олиш субъекти ёки объектнинг фаркли белгисини акс эттирувчи, фойдалана олишни идентификация қилиш воситаси. Фойдаланувчилар учун фойдалана олишни идентификация қилишнинг асосий воситаси пароль ҳисобланади.

### Идентификатор безопасности

**uz** - хавфсизлик идентификатори  
**en** - security identifier,  
**SID**

Глобальный уникальный идентификатор субъекта системы безопасности. Различают идентификаторы безопасности учетных записей и общеизвестные идентификаторы безопасности.

Хавфсизлик тизими субъектининг глобал ноёб идентификатори. Ҳисобга олинadиган ёзувларнинг хавфсизлик идентификаторлари ва ҳаммага маълум хавфсизлик идентификаторлари фарқланади.

### Идентификатор безо-

Идентификатор безопасности с фикс-

## И

**пасности общеизвестный**

**uz** - ҳаммага маълум хавфсизлик идентификатори

**en** - well-known SID

**Идентификатор диагностического сообщения**

**uz** - диагностик хабар идентификатори

**en** - diagnostic message identifier

**Идентификатор доступа**

**uz** - фойдалана олиш идентификатори

**en** - access identifier

**Идентификатор задачи**

**uz** - вазифа идентификатори

**en** - task identifier

**Идентификатор относительный**

**uz** - нисбий идентификатор

**en** - relative identifier, RID

роvanным численным значением и названием для системы защиты.

Муҳофаза тизими учун қайд қилинган сонли қийматга ва белгиланишга эга хавфсизлик идентификатори.

Код сообщения, выдаваемого системой программой в ответ на обнаруженную ошибку.

Тизим дастури томонидан аниқланган хагога жавобан бериладиган хабар коди.

Уникальный признак субъекта или объекта доступа.

Фойдалана олиш субъекти ёки объектининг ноёб белгиси.

Символьный код, приписываемый выполняющейся или готовой к выполнению задаче.

Бажариладиган ёки бажаришга тайёр вазифага бериладиган рамзий код.

Младшая часть идентификатора безопасности. В пределах домена идентификаторы безопасности имеют одинаковую старшую часть, а относительный идентификатор принимает последовательно возрастающие значения, начиная с 1000.

Хавфсизлик идентификаторининг кичик қисми. Домен доирасида хавфсизлик идентификаторлари бир хил катта қисмга эга, нисбий идентификатор эса 1000 дан бошлаб кетма-кет кўпаувчи қийматни олади.

## И

### **Идентификатор пользователя**

**uz** - фойдаланувчининг  
идентификатори  
**en** - user identifier, user  
ID

1. Последовательность символов или изображение, которое используется системой обработки данных для идентификации пользователя.
2. Персональное обозначение (имя, код и т.п.), позволяющее однозначно выделить идентифицируемый субъект (объект) среди всех других в полном множестве субъектов (объектов).
3. Символическое имя, присваиваемое отдельному лицу или группе лиц и разрешающее использование ресурсов вычислительной системы.

1. Фойдаланувчини идентификация қилиш учун маълумотларни қайта ишлаш тизимида фойдаланиладиган тасвир ёки символлар кетма-кетлиги.

2. Барча бошқа субъектлар (объектлар)-нинг тўлиқ кўплиги ўртасида идентификация қилинувчи субъект (объект)ни бир хил ажратишга имкон берадиган хусусий белгиланиш (ном, код ва ш.к.).

3. Алоҳида шахсга ёки шахслар гуруҳига бериладиган ҳамда ҳисоблаш тизими ресурсларидан фойдаланишга рухсат берадиган рамзий ном.

### **Идентификатор пользователя сети**

**uz** - тармоқдан фойдаланувчи идентификатори  
**en** - network user identifier, NUI

Уникальный код, используемый для идентификации пользователя службой коммутации пакетов.

Пакетларни коммутациялаш хизмати томони-дан фойдаланувчини идентификация қилиш учун ишлатиладиган ноёб код.

**Идентификация  
uz** - идентификация  
қилиш

1. Присвоение идентификаторов субъектам и объектам системы.
2. Присвоение субъектам и объектам



## И

en - identification

доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

3. Процесс распознавания определенных компонентов системы, обычно с помощью уникальных имен (идентификаторов), воспринимаемых системой.

4. Выяснение личности пользователя с целью предоставления ему определенного набора прав и привилегий при работе с системой, например, определение соответствующих пользователю идентификаторов безопасности.

1. Тизим субъектлари ва объектларига идентификаторлар бериш.

2. Фойдалана олиш субъектлари ва объектларига идентификатор бериш ва ёки такдим этилаётган идентификаторни ўзлаштирилган идентификаторлар рўйхати билан солиштириш.

3. Тизимнинг айрим компонентларини, одатда, тизимда қабул қилинадиган ноёб номлар (идентификаторлар) ёрдамида аниқлаш жараёни.

4. Фойдаланувчининг шахсини, унга тизим билан ишлашда ҳуқуқ ва имтиёзларнинг маълум тўпламини бериш мақсадида аниқлаш, масалан, фойдаланувчига тааллуқли хавфсизлик идентификаторини белгилаш.

**Идентификация**  
**аутентифицированная**

uz - аутентификация  
қилинган идентификация

en - authenticated  
identity

Отличительный идентификатор администратора доступа, удостоверяемый путем аутентификации.

Аутентификация қилиш йўли билан тасдиқланадиган эркин фойдаланиш маъмурининг фарқловчи идентификатори.

## И

**Идентификация терминала**

**uz** - терминални идентификация қилиш  
**en** - terminal identification

Процесс автоматической передачи на абонентский терминал установленного идентификатора, относящегося к удаленному абонентскому терминалу (терминалам), с которым (которыми) установлено соединение

Уланиш ўрнатилган узокдаги абонент терминали (терминаллари)га тааллуқли белгиланган идентификаторни абонент терминалига автоматик узатиш жараёни.

**Избыточность**

**uz** - ортиқчалик  
**en** - redundancy

Введение в систему дополнительных компонентов сверх минимально необходимого их числа с целью повышения надежности системы. Различают избыточность аппаратную, информационную, алгоритмическую.

Тизимга унинг ишончлилигини ошириш мақсадида, минимал зарур сонидан кўп бўлган қўшимча компонентларни киритиш. Аппарат, ахборот, алгоритм ортиқчалиги фарқ қилинади.

**Избыточность кода**

**uz** - коднинг ортиқчалиги  
**en** - code redundancy

Разность между средним числом битов, используемых для кодирования одного сообщения источника и минимально возможным числом битов, полученным из теоремы Шеннона.

Манбанинг бир хабарини кодлаш учун қўлланиладиган битларнинг ўртача сони ва Шеннон теоремасидан олинган битларнинг мумкин бўлган энг кам сони ўртасидаги фарқ.

**Изменение формата**

**uz** - форматни ўзгартириш

Использование нестандартного формата диска для защиты от копирования, в этом случае диск не может быть прочи-

## И

**en** - format alteration

тан стандартными утилитами копирования.

Дискнинг ностандарт форматидан нусха кўчиришдан химоя қилишда фойдаланиш, бунда дискни нусха кўчиришнинг стандарт утилиталари ўқий олмайди.

### **Имитация**

**uz** - имитация

**en** - imitation

Составная часть технической дезинформации, осуществляемая путем искусственного воспроизведения ложных объектов и технических демаскирующих признаков.

Техник ёлгон хабар тарқатишнинг таркибий қисми, сохта объектлар ва техник демаскировка қилувчи белгиларни сунъий қайта тиклаш йўли билан амалга оширилади.

### **Имитация экрана**

**uz** - экран имитацияси

**en** - screen mimic

Маскировка экрана, обычно связанная с высвечиванием ничего не подозревающему пользователю ложного экрана опроса для перехвата его имени и пароля.

Ҳеч нарсадан гумон қилмаган фойдаланувчига, унинг номи ва паролини билиб олиш учун сохта сўроқ экранини ёритиш билан боғлиқ экран маскировкаси.

### **Имитовставка**

**uz** - имитокўшимча

**en** - imitoinserter

Отрезок информации фиксированной длины, полученный по определенному правилу из открытых данных и ключа и добавленный к зашифрованным данным для обеспечения имитозащиты.

Очиқ маълумотлар ва калитдан маълум қоидага кўра олинган ҳамда шифрлан-

## И

ган маълумотларга имитомуҳофазани таъминлаш учун қўшилган, қайд қилинган узунликдаги ахборот бўлаги.

### **Имитозащита**

**uz** - имитомуҳофаза  
**en** - imitation (simulation)  
of protection

1. Аппаратные, аппаратно-программные или программные средства защиты системы шифрованной связи от навязывания ложных данных.
2. Защита системы шифрованной связи от навязывания ложных данных.

1. Шифрланган алоқа тизимини ёлғон маълумотлар мажбуран киритилишидан (қабул қилинишидан) сақлашнинг аппарат, аппарат-дастурий ёки дастурий муҳофаза воситалари.
2. Шифрланган алоқани ёлғон маълумотларнинг ортиқча ўрнашишидан муҳофаза қилиш тизими.

### **Имитостойкость**

**uz** - имитобардошлилик  
**en** - mimic resistance

Способность противостоять активным атакам со стороны злоумышленника, целью которых является навязывание ложного или подмена передаваемого сообщения или хранимых данных.

Мақсади ёлғон хабарни мажбуран киритиш (қабул қилиш) ёки узатиладиган ахборотни ёки сақланадиган маълумотларни алмаштириб қўйиш бўлган, жинояткорнинг актив хужумларига қарши тура олиш қобилияти.

### **Имя уникальное**

**uz** - ноёб ном  
**en** - distinguished name,  
DN

Текстовый идентификатор объекта в каталоге, построенном по спецификации X.500. Включает имена контейнерных объектов каталога, в которых находится данный объект, и имя самого объекта.

## И

Объектнинг X.500 спецификацияси бўйича тузилган каталогдаги матнли идентификатори. Каталогнинг, шу объект бўлган контейнерли объектлари номини ва объектнинг ўз номини ичига олади.

### **Инженерия социальная**

**uz** - ижтимоий инженерия

**en** - social engineering

Обход системы безопасности информационной системы с помощью нетехнических средств (обмана и т.д.).

Ахборот тизими хавфсизлик тизимини нотехник воситалар (алдаш ва б.к.) ёрдамида четлаб ўтиш.

### **Инсталлятор**

**uz** - инсталлятор

**en** - installer

Компьютерная программа, которая устанавливает файлы, например, приложения, драйверы, или другое программное обеспечение, на компьютер. Некоторые инсталляторы специально сделаны для установки содержащихся в них файлов; другие же являются универсальными и работают, считывая содержимое комплекта программного обеспечения, которое необходимо установить.

Файлларни, масалан, компьютерга илова, драйверлар ёки бошқа дастурий таъминотни ўрнатувчи компьютер дастури. Айрим инсталляторлар улардаги мавжуд файлларни ўрнатиш учун махсус ишланган; бошқалари универсал ҳисобланади ва ўрнатиш зарур бўлган дастурий таъминот комплектини ҳисобга олиб ишлайди.

### **Инсталляция**

**uz** - инсталляция

**en** - installation

Процесс установки программного обеспечения на компьютер конечного пользователя. Выполняется особой программой (пакетным менеджером), при-

## И

существующей в операционной системе, или входящим в состав самого программного обеспечения средством установки.

Охирги фойдаланувчининг компьютерига дастурий таъминот ўрнатиш жараёни. Операцион тизимда мавжуд бўлган алоҳида дастур (пакет менежер) томонидан ёки дастурий таъминотнинг таркибига кирувчи ўрнатиш воситасида бажарилади.

**Интерпретация**  
**uz** - интерпретация  
(талкин)  
**en** - interpretation

Анализ команд или операторов программы и немедленное их выполнение.

Командалар ёки дастур операторларининг таҳлили, уларнинг дарҳол бажарилиши.

**Интерпретация**  
**программная**  
**uz** - дастурий интерпретация  
**en** - software interpretation

Способ защиты управляющей программы от несанкционированной модификации путем загрузки ее в измененной форме с помощью кодового оптимизатора.

Кодли оптимизатор ёрдамида ўзгартирилган шаклда юклаш йўли билан бошқарувчи дастурни рухсат этилмаган ўзгартирилишдан муҳофаза қилиш усули.

**Интерфейс (в системах обработки данных)**

Определенный набор услуг, представляемых процессором.

**uz** - интерфейс (маълумотларни қайта ишлаш тизимларида)  
**en** - interface (in data processing systems)

Процессор такдим этадиган хизматларнинг маълум бир тўплами.

**Информация**

1. Сведения о фактах, событиях, про-

## И

**uz** - ахборот  
**en** - information

цессах и явлениях в некоторой предметной области, включенные в систему обработки информации, или являющиеся ее результатом в различных формах представления на различных носителях и используемые (необходимые) для оптимизации принимаемых решений в процессе управления объектами данной предметной области.

2. Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

1. Ахборотни қайта ишлаш тизимиға қиритилган ёки турли ташувчиларда турли шаклларда тақдим этишда унинг натижаси ҳисобланадиган ва ушбу предмет соҳасининг бошқарув объекти жараёнида қабул қилинадиган қарорларни оптималлаштириш учун (зарур бўлган) ишлатиладиган фактлар, воқеалар, жараёнлар ва ҳодисалар тўғрисидаги маълумотлар.

2. Тақдим этиш шаклидан қатъи назар, шахслар, предметлар, фактлар, воқеалар, ҳодисалар ва жараёнлар тўғрисидаги маълумотлар.

**Информация аутен-  
тификации**  
**uz** - аутентификация  
ахбороти  
**en** - authentication  
information

1. Информация, используемая для установления достоверности идентификационной информации, предъявленной логическим объектом.

2. Информация, используемая для установления подлинности личности, за которую выдает себя пользователь.

1. Манتيқий объект томонидан тақдим қилинган идентификацион ахборотнинг ишончлилигини аниқлаш учун фойда-

## И

ланиладиган ахборот.

2. Фойдаланувчи шахсининг ҳақиқийлигини аниқлаш учун фойдаланиладиган ахборот.

**Информация безопасности**

**uz** - хавфсизлик ахбороти

**en** - security information, SI

Информация, необходимая для реализации услуг обеспечения безопасности.

Хавфсизликни таъминлаш хизматларини амалга ошириш учун зарур бўлган ахборот.

**Информация (для процесса обработки данных)**

**uz** - ахборот (маълумотларни қайта ишлаш жараёни учун)

**en** - information (in data processing)

Любые знания о предметах, фактах, понятиях и т.д. проблемной области, которыми обмениваются пользователи системы обработки данных.

Маълумотларни қайта ишлаш тизими фойдаланувчилари алмашинадиган, муаммоли соҳа предметлари, фактлари, тушунчалари ва б.қ. ҳақидаги ҳар қандай билимлар.

**Информация документированная**

**uz** - ҳужжатлаштирилган ахборот

**en** - documented information

Информация, зафиксированная на материальном носителе и обладающая реквизитами, позволяющими ее идентифицировать.

Моддий ташувчида қайд этилган ва уни идентификация қилиш имконини берадиган реквизитларга эга ахборот.

**Информация защищаемая**

**uz** - муҳофаза қилинадиган ахборот

**en** - secured information

Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями нормативных документов или требованиями, устанавливаемыми собственником информации.

Мулкчилик предмети ҳисобланадиган ва норматив ҳужжатлар талаблари ёки



## И

ахборот эгаси томонидан белгиланадиган талабларга мувофиқ муҳофаза қилиниши керак бўлган ахборот.

**Информация  
конфиденциальная**  
**uz** - конфиденциал ахборот  
**en** - confidential  
information

1. Документированная информация, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Республики Узбекистан.

2. Информация, имеющая ограничения на право доступа к ней со стороны пользователей и, как следствие, требующая защиты от несанкционированного к ней доступа.

3. Служебная, профессиональная, промышленная, коммерческая или иная информация, правовой режим которой устанавливается ее собственником на основе законодательства и которая требует защиты.

1. Давлат сири ҳисобланадиган маълумотлар бўлмаган ҳужжатлаштирилган ахборот, ундан фойдаланиш Ўзбекистон Республикаси қонунларига мувофиқ чегараланади.

2. Фойдаланувчилар томонидан эркин фойдаланиш ҳуқуқи чекланган ва руҳсат этилмаган тарзда фойдалана олишдан муҳофаза қилиниши талаб этиладиган ахборот.

3. Хизматга оид, профессионал, саноат, тижоратга оид ёки ҳуқуқий режими эгаси томонидан қонунчиликка асосан белгиланадиган ва муҳофаза қилиниши талаб этиладиган ахборот.

**Информация некри-  
тическая (несекретная)**

1. Информация, не нуждающаяся в защите от раскрытия.

## И

**uz** - критик (махфий)  
бўлмаган ахборот  
**en** - unclassified  
information

2. Информация, которая не представляет собой государственную, служебную, коммерческую или личную тайны и может быть опубликована в открытой печати.

### **Информация персональная**

**uz** - шахсий ахборот  
**en** - private information

1. Очилишдан муҳофаза қилишга эҳтиёж бўлмаган ахборот.

2. Давлат, хизмат, тижорат сирларини ёки шахсий сирни ичига олмайдиган, очик матбуотда эълон қилиниши мумкин бўлган ахборот.

Сведения, которые не подлежат огласке. Их распространение по каналам телекоммуникаций требует соблюдения специальных мер безопасности.

### **Информация с ограниченным доступом**

**uz** - фойдаланиш  
чекланган ахборот  
**en** - restricted data

Ошкор қилиниши мумкин бўлмаган ахборот. Уларни телекоммуникация каналлари орқали тарқатиш махсус хавфсизлик чораларига риоя қилинишини талаб этади.

1. Информация, право доступа к которой ограничено установленными правилами разграничения доступа.

2. Информация, право доступа к которой ограничено установленными юридическими нормами и правилами.

1. Эркин фойдаланиш ҳуқуқи, фойдаланишни чеклашнинг белгиланган қоидаларига кўра чекланган ахборот.

2. Эркин фойдаланиш ҳуқуқи, белгиланган юридик нормалар ва қоидаларга кўра чекланган ахборот.

### **Информация чувствительная**

Информация, которая определена уполномоченным органом как нуж-

## И

**uz** - таъсирчан ахборот  
**en** - sensitive  
information

даюшаяся в защите, потому что ее раскрытие, модификация, уничтожение или сокрытие нанесет ощутимый ущерб кому-то или чему-то.

Очилиши, ўзгартирилиши, йўқ қилиниши ёки яширилиши кимгадир ёхуд нимагадир сезиларли зиён етказиши мумкин бўлганлиги учун, ваколатланган орган томонидан муҳофаза қилиниши зарур деб белгиланган ахборот.

### **Инфраструктура открытых ключей**

**uz** - очик калитлар  
инфраструктураси  
**en** - public key infrastructure, PKI

Технология передачи шифрованных данных по открытым каналам телекоммуникаций с использованием двух логически связанных ключей: открытого, который известен всем, и закрытого, который знает только определенный пользователь.

Мантиқий боғланган иккита: ҳаммага маълум бўлган очик ва фақат маълум фойдаланувчи биладиган ёпик калитлардан фойдаланиб, очик телекоммуникациялар каналлари орқали шифрланган маълумотларни узатиш технологияси.

### **Инфраструктура управления привилегиями**

**uz** - имтиёзларни  
бошқариш структураси  
**en** - privilege management infrastructure, PMI

Инфраструктура, способная поддерживать управление привилегиями при поддержке комплексной услуги авторизации и при взаимодействии с инфраструктурой открытых ключей.

Комплекс муаллифлаштириш хизмати кўмагида ҳамда очик калитлар инфраструктураси билан ўзаро ҳамкорликда имтиёзларни бошқариш таъминланган инфраструктура.

## И

**Искажение данных**  
**uz** - маълумотларнинг бузилиши  
**en** - data corruption

Случайное или умышленное нарушение целостности данных.

Маълумотлар яхлитлигининг тасодифан ёки қасддан бузилиши.

**Искажение информации**  
**uz** - ахборотнинг бузилиши  
**en** - information distortion

Случайная или преднамеренная не санкционированная модификация информации при ее обработке (передаче) техническими средствами в результате внешних воздействий (помех), сбоев в работе аппаратуры или ошибочных действий обслуживающего персонала.

Ташки таъсирлар (халакитлар), аппаратура ишидаги тўхташлар ёки хизмат кўрсатувчи персоналнинг нотўғри ҳаракатлари натижасида ахборотни техник воситалар ёрдамида қайта ишлаш (узатиш)да ахборотнинг тасодифий ёки қасддан рухсат этилмаган тарзда ўзгартирилиши.

**Использование вычислительной системы злоумышленное**  
**uz** - ҳисоблаш тизимидан қасддан фойдаланиш  
**en** - computer fraud

Любая деятельность, направленная на манипулирование информацией внутри вычислительной системы с целью личной выгоды, обычно финансовой.

Шахсий, оdatда, молиявий фойда олиш мақсадида ҳисоблаш тизими ичида ахборот билан манипуляция қилишга қаратилган ҳар қандай фаолият.

**Использование ловушек**  
**uz** - тузоклардан фойдаланиш  
**en** - entrapment

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

## И

Маълумотларни қайта ишлаш тизимига ошкора камчиликларни (заифликларни) атайин киритиш. Бузгунчи бу камчиликлардан (заифликлардан) фойдаланганда уни чалгитиш учун ёки киришга уринишларни аниқлаш учун мўлжалланган.

### **Использование объекта повторное**

**uz** - объектдан такрор фойдаланиш  
**en** - object reuse

Переназначение и повторное использование пространства памяти (например, страницы фрейма, сектора диска, магнитной ленты), которое ранее содержало в себе один или несколько объектов. Для поддержания безопасности это пространство при выделении его под новый объект не должно содержать информации о старом объекте.

Аввал бир ёки бир нечта объектни ўз ичига олган хотира майдонини (масалан, фрейм саҳифалари, диск сектори, магнит лентаси) қайта тайинлаш ва ундан такрор фойдаланиш. Хавфсизликни таъминлаш учун бу майдон, уни янги объектга ажратишда эски объект тўғрисидаги ахборотга эга бўлмаслиги керак.

### **Исправление**

**uz** - тузатиш  
**en** - correction

Внесение изменений в программу или набор данных путем обновления, добавления или удаления отдельных частей (фрагментов).

Дастурга ўзгартиришлар киритиш ёки айрим қисмлар (фрагментлар)ни янгилаш, қўшиш ёки олиб ташлаш йўли билан маълумотлар тўплаш.

### **Испытание**

**uz** - синов  
**en** - test, testing

Проверка системы или ее компонента путем реального выполнения каких-либо задач.

## И

Қандайдир вазифани аниқ бажариш йўли билан тизимни ёки унинг компонентини текшириш.

**Испытание на проникновение**  
**uz** - сукулиб киришга синаш  
**en** - penetration test

Испытание системы с целью проверки средств ее защиты (в частности, от несанкционированного доступа).

**Исследования специальные**  
**uz** - махсус тадқиқотлар  
**en** - special study

Муҳофаза қилиш воситаларини текшириш мақсадида тизимни синаб кўриш (хусусан, рухсат этилмаган тарзда фойдалана олишдан).

1. Исследования, которые проводятся на объекте эксплуатации технических средств обработки информации с целью определения соответствия системы защиты информации требованиям стандартов и других нормативных документов, а также для выработки соответствующих рекомендаций по доведению системы защиты до требуемого уровня.  
2. Деятельность по выявлению с использованием контрольноизмерительной аппаратуры возможных технических каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем и оценка соответствия защиты информации требованиям нормативных документов по защите информации.

1. Ахборотни қайта ишлаш техник воситаларини эксплуатация қилиш объектида ахборотни муҳофаза қилиш тизимининг стандартлар ва норматив ҳужжатларнинг талабларига мос келишини аниқлаш, шунингдек, муҳофаза қилиш тизимини талаб қилинадиган даражага-ча етказиш бўйича тегишли тавсиялар

## И

иншлаб чиқиш мақсадида олиб бориладиган тадқиқотлар.

2. Назорат-ўлчаш аппаратурасидан фойдаланиб, муҳофаза қилинадиган ахборот асосий ва ёрдамчи техник воситалар ҳамда тизимлардан чиқиб кетиши мумкин бўлган техник каналларни аниқлаш ва ахборотни муҳофаза қилишнинг шу мазмундаги норматив ҳужжатлар талабларига мос келишини баҳолаш бўйича фаолият.

**Источник**  
**uz** - манба  
**en** - source

Материальный объект или субъект, способный накапливать, хранить, преобразовывать и выдавать информацию в виде сообщений или сигналов различной физической природы.

Турли физик табиатдаги хабарлар ёки сигналлар кўринишидаги ахборотни тўплаш, сақлаш, ўзгартириш ва бериши мумкин бўлган моддий объект ёки субъект.

**Источник информации комбинаторный**  
**uz** - комбинатор ахборот манбаи  
**en** - combinatorial source

Источник, на выходе которого может появиться одна из последовательностей, принадлежащая заданному конечному множеству, например, множество векторов фиксированного веса Хемминга.

Чиқишида берилган чекловчи кўплика тааллуқли кетма-кетликлардан бири пайдо бўлиши мумкин бўлган манба, масалан, Хемминг қайдланган вазни векторлари тўплами.

**Источники коррелированные**  
**uz** - ўзаро боғланган

Источники, порождающие статистически зависимые последовательности символов.

## И

манбалар  
en - correlated sources

Символларнинг статистик боғлиқ кетма-кетлигини юзага келтирувчи манбалар.

**Источники угроз**  
uz - таҳдидлар манбалари  
en - threat source

Потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

Потенциал антропоген, техноген ёки табиий (стихийли) хавфсизликка бўлган таҳдидларни тарқатувчилар.

## К

**Канал**  
uz - канал  
en - channel

1. Маршрут передачи информации.
2. Часть системы телекоммуникаций, связывающая между собой источник и приемник сообщений.

1. Ахборотни узатиш маршрути.
2. Телекоммуникациялар тизимининг манба ва хабарлар қабул қилгични ўзаро боғловчи қисми.

**Канал временной скрытый**  
uz - вақтга боғлиқ бўлган канал  
en - covert timing channel

Скрытый канал, в котором один процесс передает информацию другому посредством модуляции доступа к системным ресурсам (например, времени занятости центрального процессора) таким образом, что эта модуляция может распознаваться и детектироваться другим процессом.

Яширин канал, унда бир жараён ахборотни бошқасига тизим ресурсларидан (масалан, марказий процессорнинг бандлик вақтидан) фойдаланишни модуляциялаш воситасида, бу модуляциялаш бошқа жараён томонидан аниқланиши ва детекторланиши мумкин бўладиган тарзда узатади.



## К

**Канал защищенный**  
**uz** - муҳофазаланган  
канал  
**en** - secure channel

Именованный канал между службами Netlogon компьютеров домена. При образовании защищенного канала создается ключ сеанса, применяемый для проверки подлинности передаваемых по каналу сообщений и для шифрования части передаваемой информации.

Домен компьютерларининг Netlogon хизматлари ўртасидаги номланган канал. Муҳофазаланган канални ҳосил қилишда канал бўйича узатиладиган хабарларнинг ҳақиқийлигини текшириш ва узатилаётган ахборотнинг бир қисмини шифрлаш учун қўлланиладиган сеанс калити яратилади.

**Канал с защитой целостности**  
**uz** - яхлитлик муҳофазаланган канал  
**en** - integrity-protected channel

Канал телекоммуникаций, к которому была применена услуга обеспечения безопасности.

Хавфсизликни таъминлаш хизмати қўлланилган телекоммуникациялар канали.

**Канал скрытый**  
**uz** - яширин канал  
**en** - covert channel

1. Канал передачи, который может быть использован для передачи данных способом, нарушающим политику безопасности.

2. Путь передачи информации, позволяющий двум взаимодействующим процессам обмениваться информацией способом, который нарушает системную политику безопасности.

1. Маълумотларни хавфсизлик сиёсатини бузадиган усулда узатиш учун қўлланилиши мумкин бўлган узатиш канали.

2. Ўзаро ҳамкорликда ишлайдиган икки жараёнга тизим хавфсизлик сиёсатини бузадиган ахборот алмашилиш имкони берадиган ахборот узатиш йўли.

## К

### Канал с памятью скрытый

**uz** - хотирага эга яширин канал  
**en** - covert storage channel

Скрытый канал, обеспечивающий прямую или косвенную запись в пространство памяти одним процессом и чтение этой информации другим процессом.

*Примечание: Скрытый канал с памятью обычно связан с использованием ресурсов ограниченного объема (например, секторов на диске), которые разделяются двумя субъектами с различными уровнями безопасности.*

Хотира майдонига бир жараён томонидан бевосита ёки билвосита ёзишни ва бу ахборотнинг бошқа жараён томонидан ўқилишини таъминловчи яширин канал.

*Изоҳ: Яширин канал хавфсизлик даражаси турлича бўлган шккита субъект билан ажратиладиган чекланган хажмдаги ресурслардан (масалан, дискдаги секторлардан) фойдаланиш билан боғлиқ.*

### Канал утечки информации

**uz** - ахборот чиқиб кетадиган канал  
**en** - covert channel

1. Канал коммуникации, позволяющий процессу передавать информацию путем, нарушающим безопасность системы.

2. Неконтролируемый физический путь от источника информации, выходящий за пределы объекта защиты или круга лиц, обладающих защищаемыми сведениями, посредством которого возможно неправомерное получение и/или воздействие на защищаемую информацию

1. Жараёнга ахборотни тизим хавфсизлиги бузиладиган йўл билан узатиш имконини берувчи коммуникация канали.

2. Муҳофаза объекти ёки муҳофаза қилинадиган маълумотларга эга бўлган шахслар доирасидан ташқарига чиқувчи, ахборот манбаидан бошланадиган физик йўл. Унинг воситасида муҳофаза қилина-

## К

диган ахборотни ноқонуний олиш ва ёки унга таъсир ўтказиш мумкин бўлади.

**Канал утечки информации технических**

**uz** - ахборот чиқиб кетадиган техник канал

**en** - technical convert channel

Физическая среда распространения сигналов, несущих конфиденциальную информацию, выходящая за пределы охраняемой территории.

Конфиденциал ахборотни ташувчи сигналларни тарқатишнинг кўрикланаётган ҳудуддан ташқарига чиқувчи физик муҳити.

**Кардер**

**uz** - кардер

**en** - carder

Мошенник («виртуальный вор»), занимающийся аферами с пластиковыми картами.

Пластик карталар билан боғлиқ қалбаки ишлар билан шуғулланувчи фирибгар («виртуал ўғри»).

**Карта идентификационная (кодовая)**

**uz** - идентификацион (кодли) карта

**en** - ID card (code)

Перфорированная бумажная или магнитная карта с нанесенным на ней кодовым словом (паролем), предназначенная для идентификации доступа пользователя к информационному ресурсу.

Фойдаланувчининг ахборот ресурсидан фойдалана олишини идентификация қилиш учун мўлжалланган, кодли сўз (пароль) туширилган, перфорацияланган қоғоз ёки магнит карта.

**Карта интеллектуальная**

**uz** - интеллектуал карта

**en** - smart card

Миниатюрная пластиковая карточка с расширенными функциональными возможностями, реализованная на микропроцессорной основе и используемая при работе с терминалом для идентификации личности.

Кенг функционал имкониятларга эга бўл-

## К

ган, микропроцессор асосидаги, шахсни идентификация қилиш учун терминал билан ишлашда фойдаланиладиган ихчам пластик карточка.

**Карта копирования**  
**uz** - нусха кўчириш картаси  
**en** - copy card

Электронное устройство, которое будучи включенным в компьютер, позволяет копировать защищенное программное обеспечение из оперативной памяти на диск.

Компьютерга киритилгач, муҳофазаланган дастурий таъминотни оператив хотирадан дискка кўчириш имконини берадиган электрон курилма.

**Карта с микропроцессором**  
**uz** - микропроцессорли карта  
**en** - chip card

Пластмассовая карточка типа кредитной, но имеющая встроенные запоминающее устройство и микропроцессор (или специализированную логическую схему).

Кредит карточкаси типигади, лекин ичида хотирловчи курилма ва микропроцессори (ёки ихтисослаштирилган мантикий схема) бўлган пластмасса карточка.

**Категория безопасности**  
**uz** - хавфсизлик категорияси  
**en** - security category

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

Фақат иерархик махфийлик грифини қўллашдан кўра жуда аниқ бўлган маълумотлардан эркин фойдаланишни бошқаришда қўлланиладиган нозик ахборотни ноиерархик гуруҳлаш.

**Категория безопасности информации**  
**uz** - ахборот хавфсиз-

Уровень безопасности информации, определяемый установленными нормами в зависимости от важности (ценности)

## К

лиги категорияси  
**en** - information  
security category

информации.

Ўрнатилган нормаларга кўра ахборотнинг муҳимлигига (қимматлилигига) боғлиқ ҳолда белгиланадиган ахборот хавфсизлиги даражаси.

**Категория доступа**  
**uz** - эркин фойдаланиш категорияси  
**en** - access category

Категория, присваиваемая логическим объектам, на основании которой они получают разрешение на использование ресурсов.

Мантикий объектларга бериладиган категория, унинг асосида объектлар ресурслардан фойдаланиш учун рухсат оладилар.

**Категория защиты информации**  
**uz** - ахборотни муҳофаза қилиш категорияси  
**en** - information protection category

Качественный показатель, отражающий степень важности защиты информации в выбранной шкале ценностей.

Танланган аҳамиятлилик шкаласида ахборотни муҳофаза қилиш муҳимлик даражасини ақс эттирувчи сифат кўрсаткичи.

**Категория конфиденциальности**  
**uz** - конфиденциаллик категорияси  
**en** - sensitivity

Характеристика ресурса, определяющая его ценность или значимость и способная включать в себя его уязвимость. Ресурснинг унинг муҳимлигини ёки аҳамиятлилигини белгиловчи ва ўз ичига ресурс заифлигини олиш характеристикаси.

**Категория управления доступом**  
**uz** - эркин фойдаланишни бошқариш категорияси  
**en** - access control category

Языковые элементы, предназначенные для определения правил, предохраняющих от несанкционированных операций.

Рухсат этилмаган операциялардан сакловчи қондаларни аниқлаш учун мўлжалланган тил элементлари.

## К

**Качество**  
**uz** - сифат  
**en** - quality

Совокупность свойств изделия, обуславливающих его пригодность удовлетворять определенные потребности в соответствии с его предназначениями.

*Примечание: Качество определяется показателями качества такими, как надежность, точность, полнота, быстрдействие и т. п.*

Ўзининг мўлжалланишига мувофиқ маҳсулотнинг маълум эҳтиёжларни қондиришга яроқлилигини асословчи хоссалари жами.

*Изоҳ: Сифат ишончлилиқ, аниқлиқ, тўлиқлиқ, тезкорлиқ ва ш.к. сифат кўрсаткичлари билан белгиланади.*

**Качество данных**  
**uz** - маълумотларнинг сифати  
**en** - data quality

Совокупность свойств данных, обеспечивающих их пригодность для решения определенных задач. К показателям качества данных относятся: точность, полнота, адекватность, непротиворечивость, защищенность и др.

Маълумотларнинг муайян вазифаларни бажариш учун яроқлилигини таъминловчи хоссалари жами. Аниқлиқ, тўлиқлиқ, адекватлиқ, зиддиятсизлиқ, муҳофаза қилинганлиқ маълумотларнинг сифат кўрсаткичлари ҳисобланади.

**Качество докумен-**  
**таци**  
**uz** - ҳужжатлар сифати  
**en** - documentation quality

Характеристика документации, определяемая полнотой и точностью описания программного обеспечения, наглядностью и удобочитаемостью материала, что позволяет быстро его осваивать и эффективно использовать.

Ҳужжатларнинг, дастурий таъминотнинг тўлиқ ва аниқ тавсифи, материалнинг равшан ва ўқишга қулайлиги билан бел-

## К

гиладаниган (бу уни тез ўзлаштириш ва ундан унумли фойдаланишга имкон беради) характеристикаси.

### **Квадрат Бофорта**

**uz** - Бофорт квадрати

**en** - Beaufirt square

Многоалфавитная криптосистема, аналогичная криптосистеме Вижинера. Строками квадрата являются строки квадрата Вижинера, записанные в обратном порядке. Криптосистема названа в честь адмирала Фрэнсиса Бофорта.

Вижинер криптотизимиға ўхшаш кўп алифболи криптотизим. Тескари тартибда ёзилган Вижинер квадрати сатрлари квадрат сатрлари ҳисобланади. Криптотизим адмирал Фрэнсис Бофорт шарафига номланган.

### **Квадрат Вижинера**

**uz** - Вижинер квадрати

**en** - Viginera square

Одна из наиболее известных многоалфавитных криптосистем. Квадрат Вижинера представляет собой квадратную матрицу с  $n^2$  элементами, где  $n$  – число символов используемого алфавита. Каждая строка квадрата заполняется циклическим сдвигом алфавита на один символ. Ключом шифрования является т.н. ключевое слово, которое меняется аналогично криптосистеме Цезаря от шага к шагу. Каждый столбец может быть рассмотрен как криптосистема Цезаря с ключами 0, 1, ..., 25. Так как ключевое слово обычно короче открытого текста, то оно используется периодически.

Кўп алифболи машхур криптотизимлардан бири. Вижинер квадрати  $n^2$  элементлар бўлган квадрат матрицани ифодалайди, бунда  $n$  – фойдаланиладиган алифбо символларининг сони. Квадратнинг ҳар бир сатри алифбони бир сим-

## К

волга циклик силжитиш билан тўлдирилади. Қадамдан қадамгача Цезар крипто-тизимига ўхшаш ўзгардиган калит сўз шифрлаш калити ҳисобланади. Ҳар бир устун 0, 1, ..., 25 калитлари бўлган Цезар крипто-тизими сифатида қаралиши мумкин. Калит сўз, одатда, очик матндан қисқа бўлгани учун, ундан даврий равишда фойдаланилади.

**Квадрат Полибия**  
**uz** - Полибий квадрати  
**en** - Polybius checkerboard

Одноалфавитная криптосистема, описанная греческим историком Полибием. Представляет собой квадрат 5x5. Каждый символ открытого текста заменяется на пару символов, указывающих на столбец и строку, в которых расположен символ открытого текста.

Грек тарихчиси Полибий томонидан тавсифланган бир алифболи крипто-тизим. Ўзида 5x5 квадратни ифодалайди. Очик матннинг ҳар бир симболи очик матннинг симболи жойлашган устун ва сатрни кўрсатувчи жуфт символлар билан алмаштирилади.

**Квинтет**  
**uz** - квинтет  
**en** - quintet, Q

Аутентификационный вектор в UMTS, состоящий из пяти компонентов - RAND, XRES, CK, IK и AUTN.

Бешта компонент - RAND, XRES, CK, IK ва AUTN дан ташкил топган, UMTS даги аутентификацион вектор.

**Класс защищенности**  
**uz** - муҳофаза қилинганлик классификацияси  
**en** - protection class

Определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации



## К

Ҳисоблаш техникаси (автоматлаштирилган тизим) воситаларини ахборотдан рухсат этилмаган тарзда фойдалана олишдан муҳофаза қилиш бўйича талабларнинг маълум бир йиғиндиси.

### Класс идентифика- тора

**uz** - идентификатор  
класси

**en** - naming class

Категория, определяющая способ связи идентификатора со значением и способ его использования.

Идентификаторнинг қиймат билан боғланиш ва ундан фойдаланиш усулини белгиловчи категория.

### Классификация

**uz** - классификация-  
лаш (таснифлаш)

**en** - classification

Сортировка информации по категориям безопасности.

Ахборотни хавфсизлик категориялари бўйича саралаш.

### Класс рисков

**uz** - риск (эхтимолий  
хавф)лар класси

**en** - risk category

Множество угроз информационной безопасности, выделенных по определенному признаку, например, относящихся к определенной подсистеме или типу ресурса.

Маълум бир, масалан, муайян кичик тизимга ёки ресурс турига тегишли белгига қараб ажратилган, ахборот хавфсизлигига бўладиган кўплаб таҳдидлар.

### Клонирование

**uz** - клонлаш

**en** - cloning

Изготовление сотового телефона-двойника с чужим номером путем его перепрограммирования.

Қайта дастурлаш йўли билан бегона рақамли сотали ўқшаш телефонни тайёрлаш.

### Ключ анонимности

**uz** - анонимлик кали-  
ти

Вспомогательный ключ, используемый в процедуре аутентификации через шифрование (не связан с абонентом).

## К

**en** - anonymity key

Аутентификация килиш процедурасида шифрлаш орқали фойдаланиладиган ёрдамчи калит (абонент билан боғланмаган).

### **Ключ аутентификации**

**uz** - аутентификация килиш калити

**en** - authentication key, A-KEY

1. Уникальное кодовое слово, хранящееся в памяти сотового телефона. Используется для аутентификации и генерирования ключей шифрования в сетях USDC и CDMA-450.

2. Закрытый или открытый ключ шифрования, который используется для аутентификации абонента. Каждый абонент радиосети обладает индивидуальным ключом аутентификации, запрограммированным при инициализации радиостанции.

1. Сотали телефон хотирасида сакландиган ноёб кодли сўз. USDC ва CDMA-450 тармоқларида шифрлаш калитлари ни аутентификация килиш ва генерациялаш учун ишлатилади.

2. Абонентни аутентификация килиш учун ишлатиладиган ёпиқ ёки очик шифрлаш калити. Радиотармоқнинг ҳар бир абоненти радиостанцияни инициализация килишда дастурлаштирилган индивидуал аутентификация килиш калитига эга бўлади.

### **Ключ базы данных**

**uz** - маълумотлар базаси калити

**en** - database key

Ключ, присвоенный системой управления базами данных и однозначно идентифицирующий запись базы данных.

Бошқарув тизими томонидан маълумотлар базасига берилган ва маълумотлар базаси ёзувини катъий идентификация килувчи калит.

## К

### Ключ вторичный

uz - иккиламчи калит

en - secondary key

1. Ключ, получаемый путем логического преобразования основного сообщения и какого-либо входного параметра, например, серийного номера абонентской станции.

2. Способ защиты программного обеспечения, в котором первый криптографический ключ открывает доступ ко второму ключу, являющемуся ключом для дешифрования программного обеспечения.

1. Асосий хабарни ва бирор-бир кириш параметрини, масалан, абонент станциясининг серия рақамини мантиқий қайта ўзгартириш йўли билан олинадиган калит.

2. Дастурий таъминотни муҳофаза қилиш усули, унда биринчи криптографи калит дастурий таъминотни дешифровка қилиш учун калит ҳисобланадиган иккинчи калитдан фойдалана олиш учун йўл очади.

### Ключ закрытый

uz - ёпиқ калит

en - private key

1. Один из ключей несимметричной системы шифрования. Используется при расшифровании сообщений и формировании электронной подписи.

2. Закрытая (секретная) часть пары криптографических ключей в системе шифрования с открытым ключом.

1. Носиметрик шифрлаш тизимининг калитларидан бири. Хабарларни расшифровка қилишда ва электрон имзони шакллантиришда ишлатилади.

2. Очиқ калитли шифрлаш тизимидаги жуфт криптографик калитларнинг ёпиқ (махфий) қисми.

### Ключ защиты памяти

Код, присваиваемый блоку памяти, выделенному программе, и используемый

## К

**uz** - хотирани мухофаза қилиш қалити  
**en** - protection key

для обращения программы к памяти в целях ее защиты. Должен совпадать с ключом защиты; при несовпадении задание завершается аварийно.

Дастур учун ажратилган хотира блокига берилган ва мухофаза қилиш мақсадида дастур хотирага мурожаат қилиши учун ишлатиладиган код. Мухофаза қалити билан мос қилиши керак; мос келмаганда топширик авария билан тугайди.

### Ключ (криптографический)

**uz** - қалит (криптографик)  
**en** - cryptographic key

1. Последовательность символов, управляющая операциями шифрования и дешифрования.
2. Параметр криптографического алгоритма, последовательность символов, обеспечивающая возможность шифрования и расшифрования.
3. Совокупность данных, определяющих конкретное преобразование из множества преобразований шифра

1. Шифрлаш ва дешифрлаш амалларини бошқарувчи символлар кетма-кетлиги.
2. Криптографик алгоритм параметри, шифрлаш ва дастлабки матнга ўгириш имконини таъминлайдиган символлар кетма-кетлиги.
3. Шифрнинг кўплаб алмаштиришларидан аниқ бир алмаштиришни белгиловчи маълумотлар жами.

**Ключ личный**  
**uz** - шахсий қалит  
**en** - private key

Ключ, предназначенный для дешифрования и используемый только его владельцем.

Дешифрлаш учун мўлжалланган ва фақат унинг эгаси томонидан фойдаланиладиган қалит.

## К

### Ключ общий

uz - умумий калит

en - public key

Секретный ключ в симметричной криптосистеме, совместно используемый двумя или несколькими пользователями.

Симметрик криптотизимдаги икки ёки бир нечта фойдаланувчи томонидан бир-галикда ишлатиладиган махфий калит.

### Ключ открытый

uz - очик калит

en - public key

1. Ключ, который предназначен для использования любым логическим объектом для зашифрованной связи с владельцем соответствующего личного ключа.
2. Один из ключей асимметричной системы шифрования. Он не является секретом, но вычислить по нему соответствующий закрытый ключ нельзя. Применяется для шифрования сообщений и при проверке электронной подписи.
3. Ключ, используемый в асимметричной криптосистеме и доступный всем пользователям системы.
4. Общий криптографический ключ, который доступен всем пользователям и служит для расшифровки сообщений или верификации цифровых подписей.

1. Исталган мантикий объект томонидан тегишли шахсий калит эгаси билан шифрланган алоқани очишда фойдаланиш учун мўлжалланган калит.

2. Асимметрик шифрлаш тизими калитларидан бири. У махфий ҳисобланмайди, лекин унга кўра тегишли ёпиқ калитни унга кўра ҳисоблаш мумкин эмас. Хабарларни шифрлаш ва электрон имзони текширишда қўлланилади.

3. Асимметрик криптотизимда қўлланиладиган ва тизимнинг барча фойдаланувчилари эркин фойдалана олиши учун қулай бўлган калит.

## К

4. Барча фойдаланувчилар эркин фойдалана оладиган ва хабарларни расшифровка қилиш ёки рақамли имзоларни верификация қилиш учун хизмат қиладиган умумий криптографик калит.

### **Ключ разблокирования PIN-кода**

**uz** - PIN-кодни блокировкадан бўшатиш калити  
**en** - PIN unblocking key, PUK

Специальный код в сети GSM, используемый для разблокировки SIM-карт.

GSM тармоғидаги SIM-карталарни блокировкадан бўшатиш учун ишлатиладиган махсус код.

### **Ключ раундовый**

**uz** - раунд калити  
**en** - round key

Секретный элемент, получаемый из ключа криптоалгоритма и используемый шифром Файстеля и аналогичными криптоалгоритмами на одном раунде шифрования.

Криптоалгоритм калитидан олинадиган ва шифрлашнинг бир раундида Файстел шифри ҳамда ўхшаш криптоалгоритмлар томонидан фойдаланиладиган махфий элемент.

### **Ключ сеансовый**

**uz** - сеанс калити  
**en** - session key

Криптографический ключ, используемый для шифрования в течение ограниченного промежутка времени, равного одному сеансу; после окончания передачи ключ автоматически стирается.

Бир сеансга тенг бўлган чекланган вақт оралиғида шифрлаш учун ишлатиладиган криптографик калит; узатиш тугагандан сўнг калит автоматик равишда ўчиб кетади.

### **Ключ секретный**

**uz** - махфий калит  
**en** - privacy key

1. Ключ, который предназначен для использования при шифровании и дешифровании ограниченным числом корреспондентов.

## К

2. Ключ, используемый в симметричной криптосистеме и разделяемый между объектами или субъектами, которые устанавливают защищенное взаимодействие.
3. Ключ, используемый в асимметричной криптосистеме и известный, как правило, только одному объекту системы.
4. Ключ шифрования, принадлежащий только одному абоненту и предназначенный для конфиденциального доступа к защищенным данным.
5. Ключ, значение которого система использует для определения того, должен ли защищенный ресурс быть доступным процессу, выдавшему данное значение ключа.

1. Шифрлаш ва дешифрлашда корреспондентларнинг чекланган сони фойдаланиши учун мўлжалланган калит.
2. Симметрик криптотизимда ишлатиладиган ва муҳофазаланган ўзаро ҳамкорликни ўрнатувчи объектлар ёки субъектлар ўртасида тақсимланадиган калит.
3. Асимметрик криптотизимда ишлатиладиган ва одатда, тизимнинг фақат бир объектига маълум бўлган калит.
4. Фақат бир абонентга тегишли ва муҳофазаланган маълумотлардан конфиденциал фойдалана олиш учун мўлжалланган шифрлаш калити.
5. Қийматидан, тизим муҳофазаланган ресурсдан калитнинг бу қийматини берган жараён фойдалана олиши ёки олмаслигини аниқлаш учун фойдаланиладиган калит.

**Ключ системный**  
**uz** - тизим калити  
**en** - system key

Ключ, обеспечивающий защиту системных средств от несанкционированного доступа.

## К

Тизим воситаларининг рухсат этилмаган тарзда эркин фойдаланишдан муҳофаза қилинишини таъминлайдиган калит.

**Ключ скрытый**  
**uz** - яширин калит  
**en** - sealed key

Ключ шифрования, который в явном виде не хранится на станции, а воспроизводится каждый раз с помощью криптографических алгоритмов.

Станцияда очик кўринишда сақланмайдиган, ҳар сафар криптографик алгоритмлар ёрдамида қайта ишлаб чиқиладиган шифрлаш калити.

**Ключ стойкий**  
**uz** - барқарор калит  
**en** - strong key

Ключ, длина которого достаточна для построения практически стойкой криптосистемы.

Узунлиги амалда барқарор криптотизим тузиш учун етарли бўлган калит.

**Ключ управления доступом**  
**uz** - фойдалана олишни бошқариш калити  
**en** - access control key

Значение, предъявляемое процессом системе управления базами данных и сравниваемое ею с соответствующим значением с целью предотвращения несанкционированного доступа к данным.

Жараён томонидан маълумотлар базаси бошқариш тизимига бериладиган ва маълумотлардан рухсат этилмаган тарзда эркин фойдаланишнинг олдини олиш мақсадида, тегишли қиймат билан солиштириладиган қиймат.

**Ключ целостности**  
**uz** - яхлитлик калити  
**en** - integrity key, ИК

Ключ шифрования, применяемый для защиты информации от модификации или замены либо в процессе передачи по сети.

Ахборотни ўзгартирилишдан ёки алмаштирилишдан ё тармоқ орқали узатиш



## К

жараёнида муҳофаза қилиш учун қўлла-  
ниладиган шифрлаш калити.

**Ключ шифрования**  
**uz** - шифрлаш калити  
**en** - encryption key

1. Параметр алгоритмов шифрования и расшифрования.
2. Специальным образом сформированная случайная последовательность, имеющая сравнительно небольшую длину и используемая для управления процессом шифрования.
3. Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования информации, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

1. Шифрлаш ва расшифровка қилиш алгоритмларининг параметри.
2. Нисбатан унча катта бўлмаган узунликка эга бўлган ва шифрлаш жараёнини бошқариш учун ишлатиладиган махсус шакллантирилган тасодифий кетма-кетлик.
3. Ахборотни криптографик қайта ўзгартириш алгоритми айрим параметрларининг, бу алгоритм учун мумкин бўлган ўзгартиришлар ичидан битта ўзгартириш танланишини таъминловчи аниқ махфий ҳолати.

**Книга кодировочная**  
**uz** - код китоби  
**en** - code book

Книга, используемая при преобразовании открытого текста в закодированную форму (криптограмму).

Очиқ матнни кодланган шаклга (криптограммага) айлантиришда фойдаланиладиган китоб.

**Код**  
**uz** - код

1. Множество преобразований элементов открытого текста (буквы, сочетания

## К

**en - code**

букв, слова и т.п.) группами символов (букв, цифр или других знаков). Является специальным типом шифра.

2. Правило преобразования сообщения из одного (исходного) алфавита в другой (объектный), обычно без каких-либо потерь информации.

1. Очик матн элементларини (харфлар, харфлар бирикмаси, сўз ва ш.к.) символлар гуруҳлари (харфлар, рақамлар ёки бошқа белгилар) билан кўплаб қайта ўзгартириш. Шифрнинг махсус тури ҳисобланади.

2. Хабарни бир (дастлабки) алифбодан бошқасига (объект) ахборотни ҳеч қандай йўқотишларсиз қайта ўзгартириш қоидаси.

**Код аутентификации**

**uz - аутентификация қилиш коди**

**en - authentication code**

Код фиксированной длины (имитовставка), вырабатываемый из данных с использованием секретного ключа и добавляемый к данным с целью обнаружения факта изменений хранимых или передаваемых по каналу телекоммуникаций данных.

Махфий калитдан фойдаланиб маълумотлардан олинадиган ва сақланадиган ёки телекоммуникациялар канали орқали узатиладиган маълумотларнинг ўзгартирилиш фактини аниқлаш мақсадида, маълумотларга кўшиладиган қатъий узунликдаги код (имитокўшимча).

**Код аутентификации сообщений**

**uz - хабарларни аутентификация қилиш коди**

1. Последовательность битов, являющаяся функцией обоих данных (открытого текста или шифротекста) и секретного ключа, которая присоединяется к данным, чтобы обеспечить аутентификацию данных.

## К

**en** - message authentication code, MAC

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

2. Код фиксированной длины, формируемый по заданному алгоритму из случайного входного потока и ключа шифрования.

1. Иккала маълумотнинг (очиқ матн ёки шифрланган матн) ҳамда махфий калитнинг функцияси бўлган битлар кетма-кетлиги. Маълумотларни аутентификация қилишни таъминлаш учун уларга кўшилади.

*Изоҳ: Хабарларни аутентификация қилиш кодини генерациялаш учун фойдаланиладиган функция, кўпчилик ҳолларда, бир томонлама функция ҳисобланади.*

2. Беришган алгоритм бўйича тасодифий кириш оқими ва шифрлаш калитидан тузиладиган, қайд қилинган узунликдаги код.

**Код, изменяющийся во времени**

**uz** - вақтда ўзгарувчи код  
**en** - time variant code

Код, слова которого некоторым образом изменяются в процессе работы.

Сўзлари иш жараёнида бирор-бир тарзда ўзгарадиган код.

**Код каскадный**

**uz** - каскадли код  
**en** - cascade code

Код с исправлением ошибок, который можно рассматривать как результат последовательного применения нескольких других кодов.

Бир нечта бошқа кодни кетма-кет кўллаш натижаси сифатида қаралиши мумкин бўлган хатоларни тузатувчи код.

**Код контрольный**

**uz** - назорат коди  
**en** - check code

Код, позволяющий автоматически обнаруживать, локализовать и устранять ошибки в передаваемых данных.

## К

Узатиладиган маълумотлардаги хато-ларни автоматик тарзда аниқлаш, тарқалишига йўл қўймаслик ва бартараф қилиш имконини берадиган код.

### **Код контрольный (проверочный)**

**uz** - назорат (текшириш) коди  
**en** - checking code

Машинные команды, которые читают часть диска, чтобы определить, не является ли он несанкционированной копией.

Рухсат этилмаган тарзда кўчириб олинган нухса эмаслигини аниқлаш учун дискнинг бир қисмини ўқийдиган машина командалари.

### **Код обнаружения манипуляции**

**uz** - манипуляцияни аниқлаш коди  
**en** - manipulation detection code, MDC

Последовательность битов, являющаяся функцией данных, к которым она добавлена, чтобы можно было обнаруживать наличие манипуляции.

*Примечания:*

- 1. Полученное сообщение (данные плюс код обнаружения манипуляции) может быть зашифровано, чтобы обеспечить секретность или аутентификацию данных.*
- 2. Функция, используемая для генерации кода обнаружения манипуляции, должна быть общедоступной.*

Манипуляция мавжудлигини аниқлаш мумкин бўлиши учун ўзи қўшилган маълумотларнинг функцияси бўлган битлар кетма-кетлиги.

*Изоҳлар:*

- 1. Олинган хабар (маълумотлар+манипуляцияни аниқлаш коди) маълумотларнинг махфийлигини ёки аутентификация қилинишини таъминлаш мақсадида шифрланиши мумкин.*
- 2. Манипуляцияни аниқлаш кодини генерация қилиш учун қўлланиладиган функция умум-фойдаланадиган бўлиши керак.*

### **Код операции**

**uz** - операция коди

Команда ЭВМ на уровне машинного кода.

## К

en - operation code

Машина коди даражасидаги ЭХМ командаси.

**Код с контролем на четность**

uz - жуфтликни назорат қилиш коди  
en - parity check code

Двоичный код, в котором к каждой кодовой комбинации присоединяется дополнительный контрольный разряд, что позволяет сохранить принятую в системе одну и ту же четность двоичных блоков.

**Код с минимальной избыточностью**

uz - минимал ортикчаликка эга код  
en - minimum redundancy code

Иккилик код, унда ҳар бир кодли комбинацияга қўшимча назорат разряди қўшилади, бу иккилик блокларнинг тизимда қабул қилинган айнан бир жуфтлигини сақлаш имконини беради.

Как правило, под этим подразумевается код, построенный по процедуре Хаффмана. В общем случае «оптимальный» код с точки зрения средней длины кодового слова, сложность реализации кодирования не рассматривается.

**Код с минимальным расстоянием**

uz - минимал ораликли код  
en - minimum distance code

Қоидага кўра, бунда Хаффман процедураси бўйича тузилган код тушунилади. Умумий ҳолда кодли сўзнинг ўртача узунлиги нуқтаи назаридан қараганда «оптималь» код, кодлашни амалга оширишнинг мураккаблиги кўриб чиқилмайди.

Избыточный код, в котором переход от одного допустимого значения к следующему сопровождается минимальным изменением в кодовой комбинации. Позволяет обнаруживать в передаваемых данных только одиночные ошибки.

Ортикча код, унда йўл қўйиладиган бир кийматдан кейингисига ўтиш кодли комбинациядаги минимал ўзгариш билан боради. Узатиладиган маълумотларда

## К

фақат якка хатоларни аниқлаш имконини беради.

### **Код с переменной скоростью**

**uz** - ўзгарувчан тезликли код  
**en** - variable-rate code

Код, используемый при описании сверхточных кодов, у которых длина кодовых подблоков изменяется во времени, а длина информационных подблоков остается постоянной.

### **Код установления подлинности сообщения**

**uz** - хабарнинг ҳақиқийлигини ўрнатиш коди  
**en** - message authentication code, MAC

Кодли қисм блокларнинг узунлиги вақт бўйича ўзгарадиган, ахборот қисм блокларининг узунлиги доимийлигича қоладиган юқори аниқликдаги кодларни тавсифлашда қўлланиладиган код.

Код, присоединяемый к сообщению отправителем, который является результатом обработки сообщения через процесс криптографии.

### **Код Хаффмана**

**uz** - Хаффман коди  
**en** - Huffman code

Хабарга жўнатувчи томонидан қўшила-диган, криптография жараёни орқали хабарни қайта ишлаш натижаси ҳисобланадиган код.

Префиксный код, в котором длина кодовой комбинации обратно пропорциональна частоте появления кодируемого элемента (чем чаще встречается элемент, тем короче кодовая комбинация).

### **Код Хемминга**

**uz** - Хемминг коди  
**en** - Hamming code

Префиксли код, унда кодли комбинациянинг узунлиги кодлаштириладиган элементнинг пайдо бўлиш частотасига тескари пропорционал (элемент қанча кўп учраса, кодли комбинация шунча қисқа).

Код с минимальной избыточностью, обеспечивающий исправление одиночных ошибок.

## К

Якка хатоларнинг тузатилишини таъминловчи минимал ортиқчаликка эга код.

### Кодирование

uz - кодлаш

en - coding

Процесс преобразования исходного алфавита в объектный.

Дастлабки алифбони объектли алифбога кайта ўзгартириш жараёни.

### Кодирование источника

uz - манбани кодлаш

en - source coding

Использование в рамках заданного алфавита кодов переменной длины с целью уменьшения числа символов в сообщении до минимума, необходимого для представления всей информации сообщения или по крайней мере для обеспечения условий такого сокращения.

Берилган алифбо доирасида ўзгарувчан узунликдаги кодлардан, хабардаги символлар сонини, хабардаги бутун ахборотни тақдим этиш ёки ҳеч бўлмаганда бундай қисқартириш шартларини таъминлаш учун зарур бўлган энг кам даражагача қамайтириш мақсадида фойдаланиш.

### Кодирование канальное

uz - канал бўйича

кодлаш

en - channel coding

1. Использование кодов с обнаружением ошибок или кодов с исправлением ошибок для обеспечения надежной передачи по каналу телекоммуникаций.

2. Способ передачи зашифрованных сообщений, при котором каждое сообщение дешифрируется и перекодируется вновь после каждого этапа его пересылки.

1. Телекоммуникациялар канали орқали ишончли узатишни таъминлаш учун хатоларни аниқловчи кодлардан ёки хатоларни тузатувчи кодлардан фойдаланиш.

2. Шифрланган хабарларни узатиш усули,

## К

бунда ҳар бир хабар дешифровка қилинади ва уни қайта жўнатишнинг ҳар бир босқичидан сўнг яна қайта кодланади.

**Кодирование с использованием флага**  
**uz** - байроқдан  
фойдаланиб кодлаш  
**en** - flag coding

Добавление к коду некоторой последовательности символов, которая не является кодовым словом и в процессе работы может быть использована как разделитель между словами.

**Кодирование с критерием верности**  
**uz** - ишончлилиқ критерийси билан кодлаш  
**en** - coding with fidelity criterion

Кодга кодли сўз ҳисобланмайдиган ва иш жараёнида сўзлар ўртасида бўлувчи сифатида ишлатиладиган символларнинг бирор-бир кетма-кетлигини кўшиш.

Такое преобразование сообщения источника в кодовое слово, при котором после обратного преобразования получают некоторое другое сообщение, близкое к исходному в смысле заданного критерия верности.

**Коды Боуза-Чоудхури-Хокенгема (БЧХ)**  
**uz** - Боуз-Чоудхури-Хокенгем (БЧХ) кодлари  
**en** - Bose-Chaudhuri-Nocquenghem (BCH) codes

Манба хабарини кодли сўзга қайта ўзгартириш, бунда тескари ўзгартиришдан сўнг, дастлабки хабарга берилган ишончлилиқ критерийси маъносида якин бўлган қандайдир бошқа хабар олинади.

Семейство двоичных линейных блочных кодов с исправлением ошибок. Эти коды весьма эффективны, но главное их преимущество состоит в простоте кодирования/декодирования (с использованием сдвиговых регистров). Коды БЧХ используются и в качестве циклических кодов.

Хатоларни тузатувчи иккилик чизикли блокли кодлар туркуми. Бу кодлар анча самарадор, лекин уларнинг асосий афзаллиги кодлаш/декодлашнинг оддийли-



## К

гида (силжиш регистрларидан фойдаланиб). БЧХ кодлари циклик кодлар сифатида ҳам ишлатилади.

### Коды Голея

uz - Голей кодлари

en - Golay codes

Семейство совершенных линейных блоковых кодов с исправлением ошибок. Коды Голея можно рассматривать как циклические коды.

Хатоларни тузатувчи чизикли блокли кодлар туркуми. Голей кодлари циклик код сифатида ҳам кўриб чиқилиши мумкин.

### Коды Гоппы

uz - Гопп кодлари

en - Goppa codes

Коды, исправляющие ошибки, используемые в различных криптосистемах. Использование кодов Гоппы основано на том факте, что декодирование кодов Гоппы возможно осуществить вручную, в то время как декодирование линейных блочных кодов, под которые «маскируются» коды Гоппы является NP-полной задачей и трудно выполнимо.

Турли криптотизимларда ишлатиладиган, хатоларни тузатувчи кодлар. Гопп кодларидан фойдаланиш Гопп кодларини декодлашни қўлда амалга ошириш мумкинлигига асосланган (Гопп кодлари «яширинадиган»), чизикли блокли кодларни декодлаш NP тўлиқ вазифа бўлиб, уни бажариш жуда қийин.

### Коды, исправляющие ошибки

uz - хатоларни тузатувчи кодлар

en - error-correction code

Избыточные коды, использование которых позволяет с большой вероятностью не только обнаруживать, но и исправлять возникшие при передаче информации ошибки.

Ортиқча кодлар, улардан фойдаланиш катта эҳтимоллик билан, ахборот уза-

## К

тишда содир бўладиган хатоларни нафақат аниқлаш, балки тузатиш имконини ҳам беради.

### Коды Рида-Мюллера

**uz** - Рид-Мюллер кодлари  
**en** - Reed-Muller codes, RM codes

Семейство двоичных циклических блочных кодов с исправлением ошибок. Хатоларни тузатувчи иккилик циклик блокли кодлар туркуми.

### Коды Рида-Соломона

**uz** - Рид-Соломон кодлари  
**en** - Reed-Solomon codes, RS codes

Важное семейство линейных блочных кодов с исправлением ошибок, особенно удобных для исправления пакетов ошибок. Они могут быть отнесены к циклическим кодам.

Хатоларни тузатувчи чизикли блокли кодларнинг, хатолар пакетларини тузатиш учун айниқса кулай бўлган, муҳим туркуми. Улар циклик кодларга тааллуқли бўлиши мумкин.

### Коды с повторением

**uz** - такрорланувчи кодлар  
**en** - repetition codes

Семейство совершенных циклических блочных кодов с исправлением ошибок, в котором ключевые слова формируются просто  $r$ -кратным повторением слов сообщения. Если данные коды рассматривать как коды с параметрами  $(n, k)$ , то для любого  $k$  у них  $n = rk$ .

Хатоларни тузатувчи мукамал циклик блокли кодлар туркуми, унда калит сўзлар хабардаги сўзларни  $r$  марта оддий такрорлаш билан шаклланади. Агар бу кодларни  $(n, k)$  параметрларга эга кодлар деб қаралса, уларда исталган  $k$  учун  $n = rk$  бўлади.

### Коллизия

**uz** - коллизия

Событие, при котором хэш-функции от разных сообщений совпадают.

## К

en - collision

Турли хабарларнинг хэш-функцияси бир-бирига мос келадиган ҳодиса.

**Команда перехода в режим шифрования**  
uz - шифрлаш режими  
en - ciphering mode  
command, СМС

Команда, передаваемая базовой станцией и иницирующая установление режима шифрования в мобильной станции.

**Компилятор**  
uz - компилятор  
en - compiler

Транслятор, предназначенный для выполнения компиляции.

**Комплекс средств защиты**  
uz - муҳофаза қилиш воситалари комплекси  
en - trusted computing base, ТСВ

Компиляцияни бажариш учун мўлжалланган транслятор.

Совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или систем от несанкционированного доступа к информации и к объектам отрасли связи и информатизаций.

**Комплексность защиты**  
uz - муҳофазанинг комплекслиги  
en - security complexity

Ҳисоблаш техникаси воситалари ёки тизимларининг ахборотдан ҳамда алоқа ва ахборотлаштириш соҳаси объектларидан рухсат этилмаган тарзда фойдалана олишдан муҳофаза қилинишини таъминлаш учун яратиладиган ва тутиб туриладиган дастурий ҳамда техник воситалар жами.

Принцип защиты, предусматривающий мероприятия против всех опасных видов и средств технической разведки.

Техник разведканинг барча хавфли турлари ва воситаларига қарши тадбирларни кўзда тутувчи муҳофаза қилиш принципи.

## К

### Компоновка

uz - компоновка

килиш

(жой-жойига кўйиш)

en - arrangement

Целенаправленное объединение данных или информации одной системы обработки данных с данными или информацией другой системы для получения защищенной информации.

Мухофаза килинган ахборотни олиш учун, маълумотларни қайта ишлаш битта тизимнинг ахборот ёки маълумотларини бошқа тизимнинг ахборот ёки маълумотлари билан аниқ бир мақсадни кўзлаган ҳолда бирлаштириш.

### Компрометация

uz - компрометация

(обрўсизлантириш)

en - compromise

1. Непреднамеренное раскрытие криптографических ключей или конфиденциальной информации.

2. Утеря критичной информации либо получение ее неавторизованными для этого субъектами (лицами, программами, процессами и т.д.).

3. Нарушение компьютерной безопасности, в результате чего программы или данные могут быть модифицированы, уничтожены или могут стать доступными неуполномоченным логическим объектам.

1. Криптографик калитлар ёки конфиденциал ахборотни беҳосдан очиш.

2. Критик ахборотни йўқотиш ёки унинг муаллифлаштирилмаган субъектлар (шахслар, дастурлар, жараёнлар ва б.к.) томонидан олиниши.

3. Компьютер хавфсизлигининг бузилиши, унинг натижасида дастур ёки маълумотлар ўзгартирилиши, йўқ қилиниши ёки ваколатга эга бўлмаган мантикий объектлар учун очик бўлиб қолиши мумкин.

### Компрометация

Утечка или разглашение конфиденци-

## К

### информации

uz - ахборотга путур  
етказиш (ахборотни  
обрўсизлантириш)  
en - information  
compromise

### Конверт цифровой

uz - рақамли конверт  
en - digital envelope

альной информации, либо получение ее неавторизованными субъектами.

Конфиденциал ахборотнинг чиқиб кетиши (йўқолиши) ёки ошкор бўлиши ёки муаллифлаштирилмаган субъектлар томонидан олинishi.

1. Данные, добавляемые к сообщению и позволяющие предполагаемому получателю проверять целостность содержания сообщения.

2. Механизм, в котором для шифрования сообщений используется симметричная криптосистема, а для шифрования секретных ключей – асимметричная. Таким образом, долговременный ключ принадлежит асимметричной криптосистеме, а сеансовый – симметричной криптосистеме.

1. Хабарга қўшимча қилинадиган ҳамда мўлжалланган олувчига хабар мазмунининг яхлитлигини текшириш имконини берувчи маълумотлар.

2. Хабарларни шифрлаш учун симметрик криптолизимдан, махфий калитларни шифрлаш учун эса асимметрик криптолизимдан фойдаланиладиган механизм. Шу тарзда узоқ муддатли калит асимметрик криптолизимга, сеансли калит симметрик криптолизимга тегишли бўлади.

### Контейнер

uz - контейнер  
en - container

1. Файл, предназначенный для сокрытия тайных сообщений.

2. Любая информация, предназначенная для сокрытия тайных сообщений.

1. Махфий хабарларни яшириш учун мўлжалланган файл.

## К

2. Махфий хабарларни яшириш учун мўлжалланган ҳар қандай ахборот.

### **Контрмера**

**uz** - қарши чора

**en** - countermeasure

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

Ҳаракат, қурилма, процедура, метод ёки заифлигини энг кам даражага келтириш учун мўлжалланган бошқа чора-тадбир.

### **Контроллер безопасности сети с централизованным управлением**

**uz** - марказлаштирилган тарзда бошқариладиган тармоқ хавфсизлик контроллери

**en** - centralized security controller, CSC

Способ обеспечения безопасности сети, при котором основные функции безопасности реализуются в одном узле (ячейке) сети – центральном контроллере сети.

Тармоқ хавфсизлигини таъминлаш усули, бунда асосий хавфсизлик функциялари тармоқнинг битта узелида (ячейкасида) – марказий контроллерида амалга оширилади.

### **Контроллер дисковый**

**uz** - диск контроллери

**en** - disk controller

Устройство, которое подключает к ЭВМ один или несколько дисководов и управляет их работой.

ЭҲМга битта ёки бир нечта дисководни улайдиган ва уларнинг ишини бошқарадиган қурилма.

### **Контроллер домена**

**uz** - домен контроллери

**en** - domain controller

Компьютер, на котором хранится список учетных записей домена, выполняющий проверку пароля при сквозной проверке подлинности.

Ҳақиқийликни ялпи текширишда паролнинг текширилишини бажарувчи, доменнинг ҳисобга олиш ёзувлари рўйхати сақланадиган компьютер.

## К

**Контроль**  
**uz** - назорат  
**en** - control

Совокупность действий, позволяющих получать независимый обзор и анализ системных записей и активности системы с целью установления ее текущего состояния безопасности.

Тизим хавфсизлигининг жорий ҳолатини аниқлаш мақсадида, мустақил обзор ва тизим ёзувларининг таҳлилини ҳамда тизим фаоллигини олиш имконини берувчи амаллар жами.

**Контроль битов**  
**uz** - битларни назорат қилиш  
**en** - bit counting

Метод защиты от копирования, при котором диск распознается как оригинал, если некоторая дорожка (или другая область) содержит определенное число битов.

Нусха кўчиришдан муҳофаза қилиш методи, унга кўра, йўлка (ёки бошқа соҳа) битларнинг маълум сонини ўз ичига оласа, диск оригинал сифатида аниқланади.

**Контроль данных**  
**uz** - маълумотларни назорат қилиш  
**en** - data control

Проверка достоверности и целостности данных. Различают синтаксический, семантический и прагматический контроль.

Маълумотларнинг ишончлилиги ва яхлитлигини текшириш. Синтаксис, семантик ва прагматик назорат фарқ қилинади.

**Контроль доступа**  
**uz** - фойдалана олиш-ни назорат қилиш  
**en** - access control

Процесс, который ограничивает доступ к ресурсам автоматизированной системы в соответствии с требуемой моделью защиты.

Талаб қилинадиган муҳофаза қилиш моделига мувофиқ, автоматлаштирилган тизим ресурсларидан эркин фойдаланишни чеклайдиган жараён.

## К

### Контроль дублированием

**uz** - такрорлаш  
оркали назорат  
қилиш

**en** - duplication control

Контроль двух тождественных процессов посредством сравнения их результатов. Полное совпадение результатов свидетельствует об отсутствии ошибок.

Иккита бир-бирига ўхшаш жараёни уларнинг натижаларини солиштириш воситасида назорат қилиш. Натижаларнинг тўлиқ мос келиши хатоларнинг йўқлигидан далолат беради.

### Контроль избыточным кодом продольный

**uz** - ортиқча код билан бўйлама назорат қилиш

**en** - longitudinal  
redundancy control

Метод контроля целостности данных при чтении/записи на магнитную ленту – контрольные суммы считаются для блока данных по каждой дорожке.

Ўқиш/магнит тасмага ёзишда маълумотлар яхлитлигини назорат қилиш методи, назорат суммаси ҳар бир йўлка бўйича маълумотлар блоки учун ҳисобланади.

### Контроль избыточным циклическим кодом

**uz** - ортиқча циклик код билан назорат қилиш

**en** - cyclic redundancy control, CRC

1. Один из способов автоматического контроля целостности данных при их передаче и хранении. Вычисленное с помощью разновидности полиномиального кода (т.е. по более сложным правилам, чем контрольная сумма) число помещается в конце записи в памяти, используется для контроля целостности данных при операциях чтения/записи или при передаче по каналам телекоммуникаций.

2. Способ продольного контроля данных, который обеспечивает коррекцию ошибок.

1. Маълумотларни узатиш ва сақлашда уларнинг яхлитлигини автоматик назорат қилиш усулларидан бири. Полиномиал коднинг бир тури ёрдамида



## К

ҳисобланган (яъни, назорат суммасига караганда мураккаброқ коидалар бўйича) сон хотирадаги ёзувнинг охирида жойлаштирилади, ўқиш/ёзиш операцияларида ёки телекоммуникациялар каналлари орқали узатишда маълумотларнинг яхлитлигини назорат қилиш учун фойдаланилади.

2. Маълумотларни бўйлама назорат қилиш усули, хатоларнинг тузатилишини таъминлайди.

### **Контроль качества**

**uz** - сифатни назорат қилиш

**en** - quality control

Использование методов выборки, проверки и испытания на всех уровнях разработки системы с целью выпуска бездефектного оборудования и программного обеспечения.

Тизимни ишлаб чиқишнинг барча босқичларида нуқсонсиз ускуна ва дастурий таъминот чиқариш мақсадида танлаш, текшириш ва синаш методларидан фойдаланиш.

### **Контроль нажатия клавиш**

**uz** - клавишлар босилишини назорат қилиш

**en** - keystroke verification

Определение правильности ввода данных с помощью метода повторного ввода тех же самых данных с клавиатуры.

Маълумотларнинг тўғри киритилаётганлигини айнан шу маълумотларни клавиатурадан такроран киритиш усули ёрдамида аниқлаш.

### **Контроль по избыточности**

**uz** - ортиқчалик бўйича назорат қилиш

**en** - redundancy control

Контроль, выполняемый или с помощью резервированных технических средств, или на основе избыточной информации и обеспечивающий выдачу сведений о наличии определенных ошибок.

Резервланган техник воситалар ёрдамида

## К

ёки ортиқча ахборот асосида бажариладиган ва айрим хатолар мавжудлиги ҳақида маълумотлар олинисини таъминлайдиган назорат.

**Контроль по избыточности циклический**

**uz** - ортиқчалик бўйича циклик назорат  
**en** - cyclic redundancy control, CRC

**Контроль по остатку, контроль по модулю  $n$**

**uz** - қолдиқ бўйича назорат,  $n$  модули бўйича назорат  
**en** - residue check, modulo- $n$ -check

Контроль по избыточности, в котором дополнительные цифры или символы генерируются циклическим алгоритмом.

Ортиқчалик бўйича назорат бўлиб, қўшимча рақамлар ёки символлар циклик алгоритм билан генерацияланади.

Простой метод обнаружения ошибок, основанный на анализе некоторого набора данных или участка программы. Если этот набор представляет собой совокупность блоков длиной  $m$  bit, то берется сумма по модулю  $n$ , где  $n = 2^{**}m$ , и ставится в конец набора. Позднее (например, после пересылки набора данных в другое место) можно осуществить повторное вычисление контрольной суммы; при этом будут выявлены одиночные ошибки на уровне битов. Простейшим вариантом метода ( $m = 1$ ,  $n = 2$ ) является контроль четности.

Маълумотларнинг айрим тўплами ёки дастурнинг айрим қисмини таҳлил қилишга асосланган хатоларни аниқлашнинг оддий методи. Агар бу тўплам  $m$  bit узунликдаги блоklarнинг жамини ўзида ифодаласа,  $n$  модули бўйича сумма олинди, бунда  $n = 2^{**}m$ , у тўпламнинг охирига қўйилади. Кейинчалик (масалан, маълумотлар тўплами бошқа жойга ўтказилгач) назорат суммасини такрорий ҳисоблашни амалга ошириш мумкин, бунда битлар даражасидан айрим хато-

## К

лар аниқланади. ( $m = 1, n = 2$ ) методининг оддий варианты жуфтликни назорат қилиш ҳисобланади.

### Контроль по четности поперечный

**uz** - жуфтлик бўйича кўндаланг назорат  
**en** - transverse parity check

Контроль по четности на столбце двоичных цифр, которые являются членами набора, формирующего матрицу.

Матрицани шакллантирувчи тўплам бўлаги ҳисобланадиган иккилик рақамлар устунида жуфтлик бўйича назорат қилиш.

### Контроль по четности продольный

**uz** - жуфтлик бўйича бўйлама назорат  
**en** - longitudinal parity check

Контроль по четности на строке двоичных цифр, которые являются членами набора, формирующего матрицу.

Матрицани шакллантирувчи тўплам бўлаги ҳисобланадиган иккилик рақамлар сатрида жуфтлик бўйича назорат қилиш.

### Контроль правильности

**uz** - тўғрилиқни назорат қилиш  
**en** - validity check

Любая проверка соответствия некоторого объекта установленным ограничениям. Например, если какое-либо значение элемента данных вводится программой, то обычно этой программой осуществляется проверка значения на соответствие заданному диапазону.

Қандайдир объектнинг белгиланган чеклашларга мувофиқлигини ҳар қандай текшириш. Масалан, маълумотлар элементининг бирор-бир қиймати дастур томонидан киритилса, одатда шу дастур томонидан қийматнинг берилган диапазонга мувофиқлигини текшириш амалга оширилади.

### Контроль продольный (циклический)

**uz** - бўйлама (циклик) назорат

Контроль за счет избыточности, при котором контрольная сумма вычисляется для всего блока данных, как правило, с помощью циклических кодов.

## К

**en** - longitudinal redundancy check, LRC

Ортиқчалик ҳисобига назорат қилиш, бунда назорат суммаси циклик кодлар ёрдамида бутун маълумотлар блоки учун ҳисоблаб чиқилади.

**Контроль работы с данными**

Процедура, позволяющая выявить, подвергался ли блок данных случайным или преднамеренным воздействиям.

**uz** - маълумотлар билан ишлашни назорат қилиш

Маълумотлар блоки тасодифий ёки қасдан қилинган таъсирлар остида бўлган ёки бўлмаганлигини аниқлаш имконини берадиган процедура.

**en** - manipulation detection

**Контроль средств защиты**

Инспекция системных записей и работы персонала с целью проверки функционирования систем защиты, их соответствия принятой политике безопасности и требованиям эксплуатации, а также выработки соответствующих рекомендаций.

**uz** - муҳофаза воситаларини назорат қилиш

Муҳофаза тизимларининг ишлашини, уларнинг эксплуатация қилиш талабларига ва қабул қилинган хавфсизлик сиёсатига мувофиқлигини текшириш, шунингдек, тегишли тавсияларни ишлаб чиқиш мақсадида, тизим ёзувлари ва персонал ишини назорат қилиш.

**en** - security audit

**Контроль четности**

Метод контроля данных, при котором сумма по модулю 2 двоичных единиц в машинном слове, включая контрольный разряд, должна иметь определенное значение: быть всегда четной или нечетной. Неравенство суммы этому значению говорит об ошибке в данных.

**uz** - жуфтликни назорат қилиш

**en** - parity check

Маълумотларни назорат қилиш методи, унда машина сўзидаги иккилик бирлик-

## К

ларнинг икки модули бўйича суммаси, назорат разрядини қўшган ҳолда, маълум қийматга эга бўлиши керак: ҳар доим жуфт ёки ҳар доим ток бўлиши керак. Сумманинг бу қийматга тенг келмаслиги маълумотларда хато борлигини билдиради.

### **Контроль эффективности защиты информации**

**uz** - ахборотни муҳофаза қилиш самарадорлигини назорат қилиш  
**en** - information security performance management

### **Конфиденциальность**

**uz** - конфиденциаллик  
**en** - confidentiality

Проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты.

Ахборотни муҳофаза қилиш бўйича тадбирлар самарадорлигининг белгиланган талабларга ёки муҳофаза қилиш самарадорлиги нормаларига мувофиқлигини текшириш.

1. Свойство данных, позволяющее не давать права на доступ к информации или не раскрывать ее полномочным лицам, процессам или другим логическим объектам.
2. Субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.
3. Содержание критичной информации в секрете, доступ к ней ограничен узким кругом пользователей (отдельных лиц или организаций).
4. Невозможность получения несанкционированного доступа к информации в

## К

результате перехвата и других несанкционированных действий.

1. Маълумотларнинг ваколати бўлмаган шахсларга, жараёнларга ёки бошқа мантиқий объектларга ахборотдан эркин фойдаланиш ҳуқуқини бермаслик ёки уни очмаслик имконини берувчи хусусияти.
2. Ахборотдан фойдаланиш ҳуқуқига эга субъектлар доирасига чекловлар кириштириш зарурлигини кўрсатувчи ва тизимнинг (муҳитнинг) кўрсатилган ахборотни ундан эркин фойдаланиш ҳуқуқи бўлмаган субъектлардан сир сақлаш зарурлигини таъминловчи, субъектив аниқланадиган (кўшиб ёзиладиган) ахборот характеристикаси (хусусияти).
3. Критик ахборотни сир сақлаш, ундан эркин фойдаланиш фойдаланувчилар (айрим шахслар ёки ташкилотлар)нинг тор доираси билан чекланган.
4. Тутиб олиш ва бошқа рухсат этилмаган ҳаракатлар натижасида ахборотдан рухсат этилмаган тарзда фойдалана олишнинг мумкин бўлмаслиги.

**Конфиденциальность информации**  
uz - ахборотнинг  
конфиденциаллиги  
en - information  
confidentiality

Состояние информации и ее носителей, при котором обеспечиваются предотвращение несанкционированного ознакомления с ней или несанкционированного документирования (снятия копий).

Ахборот ва уни ташувчиларнинг ҳолати, бунда у билан рухсат этилмаган тарзда танишишнинг ёки рухсат этилмаган тарзда ҳужжатлаштириш (нусха кўчириш)нинг олдини олиш таъминланади.

**Конфиденциаль-**

Услуги конфиденциальности, обеспечи-

## К

**ность трафика**

**uz** - трафикнинг конфиденциаллиги

**en** - traffic confidentiality

ваюшие защиту от анализа трафика (потока сообщений).

Трафик (хабарлар оқими) нинг таҳлилдан муҳофаза қилинишини таъминловчи конфиденциаллик хизматлари.

**Концепция диспетчера доступа**

**uz** - эркин фойдаланиш диспетчери концепцияси

**en** - reference monitor concept

Концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях субъектов к объектам.

Абстракт машинага тааллуқли, эркин фойдаланишни бошқариш концепцияси, у субъектларнинг объектларга барча мурожаатларида воситачилик қилади.

**Концепция доступа**

**uz** - эркин фойдаланиш концепцияси

**en** - access concept

Модель управления доступом, осуществляемая в абстрактной ЭВМ, которая посредничает при всех обращениях субъектов к информационным ресурсам. Существуют следующие концепции доступа: дискреционное управление, мандатное управление, многоуровневая защита.

Абстракт ЭХМда амалга ошириладиган, эркин фойдаланишни бошқариш модели, у субъектларнинг ахборот ресурсларига қиладиган барча мурожаатларида воситачилик қилади. Қуйидаги эркин фойдаланиш концепциялари мавжуд: дискрецион бошқариш, мандатли бошқариш, кўп даражали муҳофаза.

**Концепция защиты информации**

**uz** - ахборотни муҳофаза қилиш концепцияси

**en** - information security concept

Система взглядов и общих технических требований по защите информации.

Ахборотни муҳофаза қилиш бўйича қарашлар ва умумий техник талаблар тизими.

## К

### **Концепция монитора ссылок**

**uz** - ҳаволалар монитори концепцияси  
**en** - reference monitor concept

### **Концепция обеспечения информационной безопасности**

**uz** - ахборот хавфсизлигини таъминлаш концепцияси  
**en** - information security provision concept

### **Конь троянский**

**uz** - троя оти  
**en** - trojan horse

Концепция контроля доступа, базирующаяся на понятии абстрактной машины, разделяющей все попытки доступа субъектов к объектам. Находит практическую реализацию в виде ядра безопасности.

Субъектларнинг объектлардан эркин фойдаланиш йўлидаги барча уринишларини тақсимловчи абстракт машина тўшунчасига асосланувчи, эркин фойдаланишни назорат қилиш концепцияси. Хавфсизлик ядроси кўринишида амалга оширилади.

Документ, определяющий общую систему взглядов на проблему обеспечения информационной безопасности в автоматизированной системе обработки информации и путях ее решения с учетом накопленного опыта и современных тенденций ее развития. Концепция обеспечения информационной безопасности является составной частью концепции безопасности организации.

Ахборотни қайта ишлаш автоматлаштирилган тизимида ахборот хавфсизлигини таъминлаш муаммосига, уни тўпланган тажриба ва ривожланишининг замонавий тенденцияларини ҳисобга олган ҳолда ҳал қилиш йўлларига қарашларнинг умумий тизимини белгиловчи ҳужжат. Ахборот хавфсизлигини таъминлаш концепцияси ташкилот хавфсизлиги концепциясининг таркибий қисми ҳисобланади.

1. Вредоносная программа, выглядящая как функционально полезная, позволяющая производить несанкциониро-



## К

ванный сбор, фальсификацию или уничтожение данных.

2. Программа, выполняющая в дополнение к основным функциям, неописанные в документации действия. Данные действия могут использовать законные полномочия субъекта системы для осуществления несанкционированного доступа.

1. Маълумотларни рухсат этилмаган тарзда тўплаш, қалбакилаштириш ёки йўқ қилишни амалга ошириш имконини берувчи, функционал фойдали бўлиб кўринадиган зарарли дастур.

2. Асосий функцияларига кўшимча равишда хужжатларда ёзилмаган ҳаракатларни бажарувчи дастур. Бундай ҳаракатлар давомида тизим субъектининг қонуний ваколатларидан рухсат этилмаган тарзда эркин фойдаланиш мумкин.

### Копировщик побитовый

uz - битма-бит нусха

кўчирувчи

en - bit copier

Программа, предназначенная для побитового считывания информации с дисков.

Ахборотни дисклардан битма-бит ҳисоблаш учун мўлжалланган дастур.

### Корреляция взвешенная

uz - баҳоланган корреляция

ен - enhanced

correlation

Метод анализа данных, применяемый к последовательности данных в различных программах с целью надежного отделения от фоновой корреляции.

Маълумотларни таҳлил қилиш методи, турли дастурларда фонли корреляциядан ишончли ажратиш мақсадида, маълумотлар кетма-кетлигига нисбатан қўлла-нилади.

### Коэффициент сжа-

Отношение длин сообщения до и после

## К

**тия в источнике со-  
общений**

**uz** - хабарлар манбаи-  
даги зичлаш коэффи-  
циенти

**en** - source compres-  
sing factor

**Коэффициент экра-  
нирования техниче-  
ского средства обра-  
ботки информации**

**uz** - ахборотни қайта  
ишлаш техник воси-  
тасини экранлаш ко-  
эффициенти

**en** - information proc-  
essing hardware  
screening factor

его сжатого кодирования.

Хабарлар узунлигининг, уни зичлаб код-  
лашдан олдинги ва кейинги нисбати.

1. Степень ослабления воздействия  
внешних электромагнитных излучений  
на электронные элементы технического  
средства обработки информации через  
электромагнитное поле за счет соответ-  
ствующего выбора базовых несущих  
конструкций и применения других аппа-  
ратных способов защиты.

2. Степень ослабления воздействия внеш-  
них электромагнитных излучений на  
электронные элементы технического сред-  
ства обработки информации через прово-  
дящие коммуникации, гальванически под-  
ключаемые к техническому средству.

1. Базавий тутиб турувчи конструкциялар-  
ни тегишлича танлаш ва муҳофаза  
қилишининг бошқа аппарат усуллари  
қўллаш ҳисобига, электромагнит майдон  
орқали ахборотни қайта ишлаш техник  
воситаларининг электрон элементларига  
қаратилган ташқи электромагнит нурла-  
нишлар таъсирини пасайтириш даражаси.

2. Техник воситаларга гальваник улана-  
диган ўтказувчи коммуникациялар орқали  
ахборотни қайта ишлаш техник воси-  
таларининг электрон элементига қара-  
тилган ташқи электромагнит нурланиш-  
лар таъсирини пасайтириш даражаси.

**Кракер**

**uz** - кракер

Разновидность хакеров, специализи-  
рующихся в области прикладного про-

## К

en - craker

граммного обеспечения. Деятельность кракеров обычно преследует корыстные цели и связана с несанкционированным доступом к «чужой» информации, в том числе и конфиденциальной.

Амалий дастурий таъминот соҳасида ихтисослашган хакерларнинг бир тури. Кракерларнинг фаолияти, одатда, ғаразли мақсадларга йўналтирилган ва «бегона» ахборотдан, жумладан, конфиденциал ахборотдан рухсат этилмаган тарзда фойдаланиш билан боғлиқ.

**Крекинг**

uz - крекинг

en - cracking

Акт проникновения в компьютерную систему или сеть.

Компьютер тизимида ёки тармоққа сукулиб кириш ҳаракати.

**Криптоалгоритм**

uz - криптоалгоритм

en - cryptalgorithm

Алгоритм, с помощью которого осуществляется логическое преобразование исходного сообщения (открытого текста) в зашифрованную последовательность знаков.

Алгоритм, унинг ёрдамида дастлабки хабар (очик матн)ни белгиларнинг шифрланган кетма-кетлигига мантикий қайта ўзгартириш амалга оширилади.

**Криптоанализ**

uz - криптотахлил

en - cryptanalysis

1. Анализ криптографической системы и/или ее входов и выходов с целью получения чувствительной информации, включая открытый текст.

2. Наука о методах раскрытия и/или подделки данных.

3. Изучение системы защиты сообщений и/или исследование ее входных и выходных сообщений с целью выделить скры-

## К

тые переменные или истинные данные, включая исходный текст.

1. Таъсирчан ахборотни, жумладан, очик матни олиш мақсадида, криптографик тизимни ва/ёки унинг киришлари ҳамда чиқишларини таҳлил қилиш.
2. Маълумотларни очиш ва/ёки қалбакилаштириш методлари ҳақидаги фан.
3. Яширин ўзгарувчан ёки ҳақиқий маълумотларни, жумладан, дастлабки матни ажратиш мақсадида хабарларни муҳофаза қилиш тизимини ўрганиш ва/ёки унинг кириш ва чиқиш хабарларини текшириш.

**Криптоанализ  
дифференциальный**  
**uz** - дифференциал  
криптоаҳлил  
**en** - differential  
cryptanalysis

Метод криптоанализа, который может применяться для повторяющихся блочных шифров. Данный метод криптоанализа базируется на методе криптоанализа по выбранному открытому тексту и анализирует отличия между двумя открытыми текстами, зашифрованными на одном ключе. Каждому из возможных ключей назначается вероятность его «правильности» и в конечном итоге вычисляется используемый ключ.

Такорланувчи блокли шифрлар учун қўлланиладиган криптоаҳлил методи. Бу криптоаҳлил методи танланган очик матн бўйича криптоаҳлил методига асосланади ва бир калитда шифрланган икки очик матнлар ўртасидаги фарқни таҳлил қилади. Мумкин бўлган калитларнинг ҳар бирига унинг «тўғрилиги» эҳтимоли белгиланади ва пировардида фойдаланиладиган калит ҳисоблаб чиқарилади.

## К

### **Криптоанализ линейный**

**uz** - чизикли  
криптотахлил  
**en** - linear  
cryptanalysis

Метод криптоанализа, который может применяться для блочных шифров. Данный метод базируется на методе криптоанализа по известному открытому тексту.

Блокли шифрлар учун қўлланилиши мумкин бўлган криптотахлил методи. Бу криптотахлил методи маълум очик матн бўйича криптотахлил методига асосланади.

### **Криптографическая стойкость**

**uz** - криптографик  
бардошлилик  
**en** - cryptostrength

1. Характеристика шифра, определяющая его стойкость к расшифровке информации без знания ключа.

2. Свойство криптографической системы, характеризующее ее способность противостоять атакам злоумышленника, как правило, с целью получить ключ, открытое сообщение или навязать ложное сообщение.

3. Устойчивость криптографического алгоритма к его криптоанализу.

1. Шифрнинг қалитни билмасдан туриб ахборотни расшифровка қилишга бардошлилигини белгиловчи характеристикаси.

2. Криптографик тизимнинг жинояткорнинг қалитни, очик хабарни олиш ёки ёлғон хабарни киритиш мақсадида қиладиган ҳужумларига қарши тура олиш қобилиятини тавсифловчи хоссаси.

3. Криптографик алгоритмнинг криптотахлилга бардошлилиги.

### **Криптография**

**uz** - криптография  
**en** - cryptography

1. Дисциплина, охватывающая принципы, средства и методы преобразования данных для сокрытия их семантического содержания, предотвращения их несанкционированного использования или обнаруживаемой модификации.

## К

2. Наука о методах обеспечения секретности и/или подлинности данных при их передаче по каналам телекоммуникаций или хранении.

3. Принципы, средства и методы преобразования информации к непонятному виду, а также восстановления информации к виду, пригодному для восприятия.

1. Маълумотларнинг семантик мазмунини яшириш, улардан рухсат этилмаган тарзда фойдаланиш ёки уларнинг аниқлаб бўлмайдиган ўзгартирилишининг олдини олиш мақсадида, маълумотларни ўзгартириш принциплари, воситалари ва методларини қамраб олувчи фан.

2. Телекоммуникациялар каналлари орқали узатишда ёки саклашда, маълумотларнинг махфийлиги ва ёки ҳақиқийлигини таъминлаш методлари ҳақидаги фан.

3. Ахборотни тушунарсиз кўринишга келтириш принциплари, воситалари ва методлари, шунингдек, уни қабул қилиш учун яроқли кўринишга қайта тиклаш.

### Криптография

#### квантовая

uz - квант криптографияси

en - quantum cryptography

Криптографический механизм, заключающийся в использовании принципов квантовой физики. Для передачи сообщений используются фотоны, что позволяет гарантировать невозможность со стороны криптоаналитика модификации информации или нарушения процесса ее передачи. В настоящий момент практического применения квантовая криптография не имеет — она используется только в качестве эксперимента.

Квант физикаси принципларидан фойдаланишга асосланган криптографик механизм. Хабарларни узатиш учун фотонлар-

дан фойдаланилади, бу криптоаналитик томонидан ахборотни ўзгартириш ёки уни узатиш жараёнини бузиш мумкин бўлмаслигини кафолатлайди. Ҳозирги вақтда квант криптографияси қўлланилмайди; фақат эксперимент сифатида ишлатилади.

### **Криптография многоуровневая**

**uz** - кўп даражали  
криптография  
**en** - multilevel  
cryptography

Механизм, который заключается в специальном методе построения криптографических ключей для симметричных криптосистем. Криптосистема, реализующая данный механизм, устроена так, что первый криптографический ключ может быть выбран произвольно, в то время как выбор всех последующих ключей должен подчиняться определенному закону.

Симметрик криптоотизимлар учун криптографик калитларни тузишнинг махсус методидан иборат механизм. Ушбу механизмни амалга оширувчи криптоотизим, кейинги калитларнинг барчасини танлаш маълум қонунга бўйсунуши керак бўлган вақтда биринчи криптографик калит ихтиёрий танланиши мумкин бўлган тарзда тузилган.

### **Криптография на эллиптических кри- вых**

**uz** - эллиптик эгри  
чизик асосидаги  
криптография  
**en** - elliptic-curve cryptography, ECC

Быстро развивающееся направление асимметричного шифрования и электронной цифровой подписи. В ECC все вычисления (например, выбор значения ключа) производятся над точками эллиптической кривой, т.е., например, вместо обычного сложения двух чисел выполняется по определенным правилам сложение двух точек кривой, при этом в качестве результата получается третья точка.

## К

Асимметрик шифрлаш ва электрон рақамли имзонинг тез ривожланиб бораётган йўналиши. ЕСС да барча ҳисоблашлар (масалан, калитнинг қийматини танлаш) эллиптик эгри чизик нукталари устида амалга оширилади, яъни, масалан, иккита сонни оддий кўшиш ўрнига, маълум қоидаларга кўра эгри чизикнинг икки нуктасини кўшиш бажарилади, бунда натижа сифатида учинчи нукта олинади.

### **Криптография с открытым ключом**

**uz** - очик калитли  
криптография  
**en** - public-key  
cryptography

1. 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.*

2. Метод шифрования, использующий пару ключей, один из которых является открытым, а второй – секретным.

1. Шифрлаш ва дешифрлаш учун очик калит каби унга мос келадиган шахсий калитдан фойдаланиладиган криптография.

*Изоҳ: Агар очик калит шифрлаш учун фойдаланилса, унга мос келадиган шахсий калитдан дешифрлаш учун фойдаланилади ва аксинча.*

2. Бири очик, иккинчиси ёпиқ бўлган жуфт калитлардан фойдаланиладиган шифрлаш методи.

### **Криптография симметричная**

**uz** - симметрик крип-  
тография  
**en** - symmetric

Криптография, в которой для шифрования и дешифрования используется один и тот же ключ.

Шифрлаш ва дешифрлаш учун битта



## К

cryptography

калитдан фойдаланиладиган криптография.

**Криптология**

uz - криптология

en - cryptology

Наука о создании и анализе систем безопасного хранения и передаче информации по каналам связи. Криптологию принято делить на две части – криптографию и криптоанализ.

Ахборотни хавфсиз сақлаш ва алоқа каналлари бўйлаб узатиш тизимини яратиш ҳамда таҳлил қилиш ҳақидаги фан. Криптология икки қисмга – криптография ва криптоанализга бўлинади.

**Криптосистема**

uz - криптотизим

en - cryptosystem

1. Совокупность используемых документов, устройств, оборудования и методов, обеспечивающая шифрование или дешифрование.

2. Совокупность организационных, технических и программных средств, обеспечивающих криптографическое преобразование информации и (или) управление, в том числе автоматизированное, процессом изготовления и распределения криптографических ключей.

1. Шифрлаш ёки дешифрлашни таъминлашда фойдаланиладиган ҳужжатлар, қурилмалар, ускуналар ва методлар жами.

2. Ахборотнинг криптографик ўзгартирилишини ва (ёки) криптографик калитларни тайёрлаш ва таксимлаш жараёни бошқарилишини, жумладан, автоматлаштирилган тарзда, таъминловчи ташкилий, техник ва дастурий воситалар жами.

**Криптосистема Габидулина**

uz - Габидулин крип-

Криптосистема, основанная на кодах, исправляющих ошибки в ранговой метрике.

## К

тотизими  
**en** - Gabidulin's  
cryptosystem

**Криптосистема  
Крука**  
**uz** - Крук крипто-  
тотизими  
**en** - Crook's  
cryptosystem

**Криптосистема Мак  
Эллиса**  
**uz** - Мак Эллис крип-  
тотизими  
**en** - Mac Alice  
cryptosystem

**Криптосистема  
Нидеррайтера**  
**uz** - Нидеррайтер  
криптотизими  
**en** - Nidderrighter's  
cryptosystem

**Криптосистема по-  
токовая самосин-  
хронизирующаяся**  
**uz** - Ёз-Ёзидан син-  
хронланувчи оқимли  
криптотизим  
**en** - data-flow

Ранг (даража) метрикасида хатоларни тузатувчи кодларга асосланган крипто-тотизим.

Криптосистема, основанная на кодах, исправляющих ошибки. В ней устранены недостатки криптосистемы МакЭллиса.

Хатоларни тузатувчи кодларга асосланган крипто-тотизим. Унда Мак Эллис крипто-тотизимининг камчиликлари бартараф қилинган.

Криптосистема, основанная на кодах, исправляющих ошибки. Ей присущи два недостатка: большая длина ключа и большая избыточность (длина шифротекста вдвое превышает длину сообщения).

Хатоларни тузатувчи кодларга асосланган крипто-тотизим. Унинг ёзига хос икки камчилиги бор: калит узунлигининг катта бўлиши ва катта ортикчалик (шифр матн узунлиги хабар узунлигидан икки марта ошади).

Криптосистема, основанная на кодах, исправляющих ошибки.

Хатоларни тузатувчи кодларга асосланган крипто-тотизим.

Потоковая криптосистема, характеризуемая тем, что каждый знак ключевого потока в любой момент времени определяется фиксированным числом предшествующих знаков шифротекста.

Калит оқимининг ҳар бир белгиси

## К

selfsynchronizing  
cryptosystem

### **Криптосистема потоковая синхронизирующаяся**

**uz** - синхронланувчи оқимли криптотизим  
**en** - data-flow  
synchronizing cryptosystem

вақтнинг исталган ониди шифр матн олдинги белгиларининг қайд қилинган сони орқали аниқланиши билан тавсифланадиган оқимли криптотизим.

Потоковая криптосистема, в которой ключевой поток вырабатывается независимо от открытого текста и шифротекста. Если какой-либо символ шифротекста потерян при передаче, то получатель должен пересинхронизировать свой ключевой поток, отбросив соответствующий символ ключевого потока для правильного расшифрования последующих знаков шифротекста.

Калит оқими очик матн ва шифр матнга боғлиқ бўлмаган тарзда ишлаб чиқиладиган оқим криптотизими. Шифр матнининг бирор-бир симболи узатишда йўқолган бўлса, олувчи шифр матнининг кейинги белгиларини тўғри расшифровка қилиш учун, калит оқимининг тегишли символини олиб ташлаб, ўзининг калит оқимини қайта синхронлаши керак.

### **Криптосистема с эллиптическими кривыми**

**uz** - эллиптик эгри чизикли криптотизим  
**en** - cryptosystem with elliptic curve

Криптосистема, основанная на математическом аппарате эллиптических кривых из теории чисел.

Сонлар назариясидан олинган эллиптик эгри чизикларнинг математик аппарати га асосланган криптотизим.

### **Криптосистема с временным раскрытием**

**uz** - вақтга қараб очиладиган криптотизим  
**en** - cryptosystem with

Криптографическая система, которая позволяет расшифровать защищенное сообщение только по истечении заданного интервала времени. В настоящий момент существует два варианта реализации таких систем:

## К

temporary disclosure

– шарады с временным замком;  
– использование доверенных агентов, принимающих на себя обязательства не раскрывать информацию в течение заданного интервала времени.

В случае использования агентов возникает проблема доверия к ним, которая может быть частично решена за счет применения механизма разделения секретов.

Факат берилган вақт интервали тугагандан сўнг муҳофазаланган ахборотни расшифровка қилиш имконини берадиган криптографик тизим. Ҳозирги вақтда бундай тизимларни амалга оширишнинг икки варианты мавжуд:

– вақтинчалик кулфловчи шарадалар;  
– берилган вақт интервали мобайнида ахборотни очмаслик мажбуриятини зиммасига олган ишончли агентлардан фойдаланиш. Агентлардан фойдаланишга тўғри келганда уларга нисбатан ишонч муаммоси юзага келади, буни сирларни тақсимлаш механизмини қўллаш ҳисобига қисман ҳал қилиш мумкин.

**Криптосистема с  
открытым ключом**  
uz - очик калитли  
криптотизим  
en - public key  
cryptosystem

Криптографическая система, в которой используется два ключа: секретный и открытый, причем ни один из ключей не может быть вычислен из другого за приемлемое время. Секретный ключ должен содержаться в тайне, в то время как открытый ключ может быть разослан всем абонентам, с которыми осуществляется взаимодействие. Такие криптосистемы также называются двуключевыми и асимметричными. Одним из основных применений таких систем является управление ключами и создание электронной цифровой подписи.

## К

Иккита – махфий ва очик калитдан фойдаланиладиган криптографик тизим. Шунингдек, калитларнинг бирортаси ҳам мақбул вақт ичида бошқасидан ҳисоблаб чиқарилиши мумкин эмас. Махфий калит сир сакланиши керак, очик калит ўзаро ҳамкорлик қилинадиган барча абонентларга юборилиши мумкин. Бундай криптотизимлар, шунингдек, икки калитли ва асимметрик криптотизимлар деб ҳам номланади. Бундай тизимлар калитларни бошқаришда ва электрон ракамли имзони яратишда қўлланилади.

**Криптосистема с секретным ключом**  
**uz** - махфий калитли  
криптотизим  
**en** - private key  
cryptosystem

Криптографическая система, в которой один и тот же криптографический ключ используется для зашифрования и расшифрования информации. Такие криптосистемы также называются одноключевыми, симметричными, обычными, двусторонними или классическими. Криптографические системы с секретным ключом делятся на блочные и поточные криптосистемы.

Криптографик тизим, бунда айнан битта криптографик калитдан ахборотни шифрлаш ва расшифровка қилиш учун фойдаланилади. Бундай криптотизимлар бир калитли, симметрик, оддий, икки томонлама ёки классик деб ҳам аталади. Махфий калитли криптографик тизимлар блокли ва оқимли криптотизимларга бўлинади.

**Критичность (1)**  
**uz** - критиклик  
**en** - criticality

Требования к достаточности определенной информации или ресурсов, обрабатывающих информацию, для ведения дел.

## К

Ишларни юритиш учун, муайян ахборот ёки ах-боротни қайта ишловчи ресурсларнинг етарлилигига қўйиладиган талаблар.

### **Критичность (2)**

**uz** - критиклик

**en** - criticalness

Характеристика ресурса, которая косвенно выражает его значение или важность.

Ресурснинг унинг аҳамиятини ёки муҳимлигини билвосита ифодаладиган характеристикаси.

### **Кэширование паролей**

**uz** - паролларни кэш-лаш

**en** - password caching

Хранение паролей и других сведений о пользователе на локальном компьютере.

Локал компьютерда паролларни ва фойдаланувчи ҳақидаги бошқа маълумотларни сақлаш.

## Л

### **«Лечение» вируса**

**uz** - вирусни «даволаш»

**en** - virus treatment

Процесс удаления вируса из зараженного им объекта и восстановления состояния этого объекта (файла, загрузочной части диска и т.д.), существовавшего до заражения вирусом.

Зарарланган объектдан вирусни чиқариб ташлаш ва бу объектнинг (файлнинг, диск юкланадиган қисмининг) вирус билан зарарлангунга қадар бўлган ҳолатини тиклаш жараёни.

### **Лицензиар в области защиты информации**

**uz** - ахборотни муҳофаза қилиш соҳасидаги лицензиар

**en** - licensor in the

Сторона в лицензионном соглашении, передающая право на проведение работ в области защиты информации.

Лицензия келишувидаги, ахборотни муҳофаза қилиш соҳасида ишларни олиб бориш ҳуқуқини берадиган томон.

## Л

information protec-  
tion field

**Лицензиат в области защиты информации**

**uz** - ахборотни муҳофаза қилиш соҳасидаги лицензиат

**en** - licensee in the information protection field

**Лицензирование**

**uz** - лицензиялаш

**en** - licensing

**Лицензирование в области защиты информации**

**uz** - ахборотни муҳофаза қилиш соҳасида лицензиялаш

**en** - licensing in the information protection field

**Лицензирование обязательное**

**uz** - мажбурий лицензиялаш

**en** - compulsory licence

Сторона в лицензионном соглашении, получившая право на проведение работ в области защиты информации.

Лицензия келишувидаги ахборотни муҳофаза қилиш соҳасида ишларни олиб бориш ҳуқуқини оладиган томон.

Деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации.

Ахборотни муҳофаза қилиш соҳасида ишларни олиб бориш ҳуқуқини бериш ёки олишдан иборат фаолият.

Деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации, оформленная лицензионным соглашением (договором), и осуществлении контроля за лицензиатом.

Лицензия келишуви (шартномаси) билан расмийлаштирилган, ахборотни муҳофаза қилиш соҳасида ишларни олиб бориш ҳуқуқини бериш ёки олишда лицензиат устидан назоратни амалга оширишда ифодаланадиган фаолият.

Юридическое постановление, которое требует от любого лица получить лицензию на определенный срок независимо от того, желает или нет лицо, выдающее лицензии, предоставить ее.

Ҳар бир шахсдан, лицензияни берадиган

## Л

шахс уни такдим этишни хохлаш ёки хохламаслигидан қатъи назар, лицензия олишни талаб этадиган юридик қарор.

### Лицензия

uz - лицензия

en - license

1. Разрешение, выдаваемое государственными органами, на право продажи или предоставления услуг.

2. Оформленный документ на право владения собственностью.

3. Оформленное соответствующим образом разрешение на право проведения тех или иных работ в области защиты информации.

1. Давлат органлари томонидан хизматларни сотиш ёки такдим этиш ҳуқуқини берувчи рухсат.

2. Мулкчиликка эгалик қилиш ҳуқуқини берадиган расмийлаштирилган ҳужжат.

3. Ахборотни муҳофаза қилиш соҳасида у ёки бу ишларни олиб бориш ҳуқуқи учун берилган, тегишли равишда расмийлаштирилган рухсатнома.

### Лицензия свободная

uz - эркин лицензия

en - free license

Открытая публикация программы в журнале, книге или частном сообщении, равносильная разрешению на использование.

Дастурнинг фойдаланиш учун рухсатга тенг журнал, китоб ёки хусусий хабарда очик эълон қилиниши.

### Лицензия упакованная

uz - жойланган лицензия

en - shrink-wrap license

Лицензия на программный продукт, доступная для чтения и вступающая в силу при вскрытии упаковки программного продукта.

Дастурий маҳсулот учун берилган, ўқиш учун қулай бўлган ва дастурий маҳсулот ўрами очилганда кучга кирадиган лицензия.

### Лицензия установочная

Лицензия на множественное копирование программного средства.



## Л

**uz** - йўл-йўрик кўрсатувчи лицензия  
**en** - site license

**Ловушка**  
**uz** - тузок  
**en** - honeypot, penetration entrapment

**Ловушка сброса**  
**uz** - чиқариб ташлаш тузоғи  
**en** - reset trapping

**Люк**  
**uz** - люк  
**en** - trapdoor

Дастурий воситадан кўплаб нусха кўчириш учун бериладиган лицензия.

Программа, которая эмулирует работу определенных сервисов (почтовых, telnet и т.п.) на компьютере, тщательно протоколирующем при этом любые действия злоумышленника.

Жинояткорнинг ҳар қандай ҳаракатини синчиклаб протоколлаштирадиган компьютердаги маълум сервислар (почта, telnet ва ш.ў.) ишини тезлаштирадиган дастур.

Программный способ отвести любую попытку прерывания штатной работы компьютера, чтобы избежать возврата управления пользователю.

Бошқарувнинг фойдаланувчига қайтишининг олдини олиш мақсадида, компьютернинг штат режимида ишлашини бузадиган ҳар қандай уринишни йўққа чиқаришнинг дастурий усули.

1. Скрытый программный или аппаратный механизм, обычно создаваемый для тестирования и поиска неисправностей, который позволяет обойти механизмы компьютерной безопасности.
2. Скрытая или недокументированная точка входа в автоматизированную систему. Может применяться для обхода системы защиты.
3. Блок, скрытый в большой программе, который разрешает пользователю преодолеть систему защиты или позволяет использовать ресурсы системы в штатном режиме.

## Л

1. Компьютер хавфсизлиги механизмларини четлаб ўтиш имконини берувчи, асосан тестлаш ва носозликларни излаб топиш учун яратиладиган яширин дастурий ёки аппарат механизм.
2. Автоматлаштирилган тизимга киришнинг яширин ёки хужжатлаштирилган нуктаси. Муҳофаза тизимини четлаб ўтишда қўллаш мумкин.
3. Катта дастурга яширинган, фойдаланувчига муҳофаза тизимидан ўтишга рухсат берадиган ёки тизим ресурсларидан штат режимида фойдаланиш имконини берадиган блок.

**Люк эксплуатационный**  
**uz** - эксплуатацион люк  
**en** - maintenance hatch

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

Дастурий таъминотдаги люк, дастурга хужжатлаштирилмаган нукталардан ёки одатдаги текширувларсиз кириш учун кўшимча имкониятларни тақдим этган ҳолда хизмат кўрсатишни енгиллаштиради.

## М

**Макровирус**  
**uz** - макровирус  
**en** - macro-virus

Файловый вирус, существующий в виде макрокоманды для определенного приложения. При открытии зараженного файла вирус прикрепляет себя к приложению и заражает все файлы, к которым обращается программа.

Маълум бир илова (дастур) учун макрокоманда кўринишида мавжуд бўлган файл вирусиди. Зарарланган файл очилганда вирусиди.

## М

иловага ёпишиб, дастур мурожаат қиладиган барча файлларни зарарлайди.

### Мандат

uz - мандат

en - ticket

1. Представление одного или нескольких прав на доступ к объекту. Мандат является разрешением на доступ.

2. Элемент матрицы доступа, определяющий тип доступа определенного субъекта к определенному объекту. Каждый раз мандат выдается субъекту динамически – при запросе доступа. Поскольку распространение мандатов происходит очень динамично, и они могут размещаться непосредственно внутри объектов, то вследствие этого контроль за ним очень затруднен. В чистом виде этот механизм используется редко. Однако реализация других механизмов контроля доступа часто осуществляется с помощью мандатов.

1. Объектдан эркин фойдаланиш учун битта ёки бир нечта ҳуқуқларни тақдим этиш. Мандат эркин фойдаланишга руҳсат бериш ҳисобланади.

2. Маълум субъектнинг маълум объектдан фойдаланиш турини белгиловчи, эркин фойдаланиш матрицаси элементи. Ҳар сафар мандат субъектга динамик равишда – эркин фойдаланиш сўралганда берилади. Мандатларни тарқатиш жуда ҳам ўзгарувчан тарзда юз бериши сабабли, улар бевосита объектлар ичида жойлашиши мумкин, бунинг оқибатида уларни назорат қилиш жуда ҳам қийин. Соф кўринишда бу механизмдан жуда кам фойдаланилади. Бироқ эркин фойдаланишни назорат қилишнинг бошқа механизмлари кўпинча мандатлар ёрдамида амалга оширилади.

## М

### **Мандат (1)**

uz - мандат  
en - capability

Представимая форма полномочия, обладание которой подтверждает право на доступ к ресурсу системы.

Такдим этиладиган ваколат шакли, унга эгалик қилиш тизим ресурсидан эркин фойдаланиш ҳуқуқини тасдиқлайди.

### **Мандат (2)**

uz - мандат  
en - credentials

Информация, передаваемая для подтверждения требуемой идентичности какого-либо объекта.

Қандайдир объектнинг талаб этиладиган идентиклигини (ўхшашлигини) тасдиқлаш учун узатиладиган ахборот.

### **Маркер**

uz - маркер  
en - token

1. Электронный носитель содержания.  
2. Короткий код для представления распознаваемых слов, например, служебных слов языка, констант и т.п.

1. Электрон мазмун ташувчи.  
2. Аниқланадиган сўзларни, масалан, тилнинг хизматга оид сўзларини, константаларни ва ш.к., такдим этиш учун мўлжалланган қисқа код.

### **Маркер безопасности**

uz - хавфсизлик маркери  
en - security token

Набор данных, передаваемых между объектами телекоммуникаций, который защищен одной или несколькими услугами безопасности, вместе с информацией безопасности, которая используется при их предоставлении.

Телекоммуникациялар объектлари ўртасида узатиладиган, маълумотларни такдим этишда фойдаланиладиган хавфсизлик ахбороти билан бирга бир ёки бир нечта хавфсизлик хизмати томонидан муҳофазаланган, маълумотлар тўплами.

## М

### **Маркер доступа**

**uz** - фойдалана олиш маркери

**en** - access token

Структура данных, связанная с процессом и являющаяся его «пропуском» к ресурсам операционной системы. В частности, включает все идентификаторы безопасности запустившего процесс пользователя.

Жараён билан боғлиқ ва унинг операцион тизим ресурсларидан фойдалана Олиши учун «рухсатномаси» ҳисобланадиган маълумотлар структураси. Хусусан, жараёни ишга туширган фойдаланувчининг барча хавфсизлик идентификаторларини ўз ичига олади.

### **Маркировка по времени**

**uz** - вақт бўйича белги қўйиш

**en** - time stamping

Метод защиты информации от ее замены или модификации в процессе передачи, основанный на включении в каждое сообщение временных меток, однозначно связанных с данными.

Ахборотни узатиш жараёнида алмаштирилиш ёки ўзгартирилишдан муҳофаза қилиш методи. Ҳар бир хабарга маълумотлар билан қатъий боғлиқ бўлган вақтинчалик белгиларни киритишга асосланади.

### **Маршрут достоверный**

**uz** - ишончли маршрут

**en** - trusted path

Механизм, с помощью которого пользователь за терминалом может взаимодействовать непосредственно с достоверной вычислительной базой (ДВБ). Он может быть активизирован только пользователем или ДВБ, его работа не может быть прервана, имитирована или нарушена недостоверным программным обеспечением.

Фойдаланувчи терминалдан кейин ишончли ҳисоблаш базаси (ИХБ) билан

## М

бевосита биргаликда ишлаши мумкин бўлган механизм. У фақат фойдаланувчи ёки ИХБ томонидан активлаштирилиши мумкин, унинг иши ишончсиз дастурий таъминот билан тўхтатилиши, имитация қилиниши ёки бузилиши мумкин эмас.

### **Маска доступа**

**uz** - фойдалана олиш  
ниқоби

**en** - access mask

Двоичное число, отдельные биты которого соответствуют разным типам доступа.

Айрим битлари фойдалана олишнинг турли типларига мос келадиган иккилик сон.

### **Маскарад**

**uz** - маскарад  
**en** - masquerade

1. Попытка какого-либо логического объекта выдать себя за другой логический объект для получения несанкционированного доступа.

2. Попытка получить доступ к системе, объекту или выполнение других действий субъектом, не обладающим полномочиями на соответствующее действие и выдающим себя за другого, которому эти действия разрешены.

3. Попытка несанкционированного проникновения в сеть путем имитации работы какого-либо легитимного пользователя.

1. Рухсат этилмаган тарзда фойдалана олиш учун бирор-бир мантикий объектнинг ўзини бошқа мантикий объект қилиб кўрсатишга уриниши.

2. Тегишли ҳаракатларни амалга оширишга ваколатлари бўлмаган ва ўзини бу ҳаракатлар рухсат берилган бошқа шахс қилиб кўрсатадиган субъект томонидан тизимдан, объектдан эркин фойдаланишга уриниш ёки бошқа ҳаракатларнинг бажарилиши.

## М

3. Қандайдир қонуний фойдаланувчининг ишини имитация қилиш йўли билан тармокка рухсат этилмаган тарзда киришга уриниш.

### **Маскиратор**

**uz** - маскиратор

**en** - maskirator

Средство защиты информации, реализующее математический алгоритм преобразования информации, не использующее секретного ключа или передающее (хранящее) его вместе с сообщением.

Ахборотни ўзгартиришнинг математик алгоритмини амалга оширадиган, махфий калитдан фойдаланмайдиган ёки уни хабар билан бирга узатадиган (саклайдиган) ахборотни муҳофаза қилиш воситаси.

### **Маскировка**

**uz** - никоблаш

**en** - masking

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

Объектларни муҳофаза қилиш методи, объектни жинояткорлар учун эгаллаб бўлмайдиган (яширин) ёки кириш қийин бўладиган ҳолатга олиб келадиган ҳаракатлардан фойдаланишга асосланган.

### **Матрица доступа**

**uz** - фойдалана олиш

матрицаси

**en** - access matrix

1. Таблица, отображающая правила разграничения доступа и предназначенная для описания свойств избирательного доступа. Представляет собой матрицу, в которой объекту системы соответствует столбец, а субъекту – строка. На пересечении столбца и строки матрицы указывается права доступа субъекта к объекту.  
2. Таблица, отображающая правила доступа субъектов к информационным ре-

## М

сурсам, данные о которых хранятся в диспетчере доступа.

3. Системная структура данных, представленная в виде таблицы, столбцы которой помечены идентификаторами всех существующих в системе ресурсов, а строки — идентификаторами всех зарегистрированных в системе пользователей. На пересечении каждого столбца таблицы с каждой ее строкой администратором системы представляется специальный указатель разрешенного конкретному пользователю типа доступа к данному объекту.

1. Кириш эрки (фойдаланиш)ни чеклаш хукукини акс этирувчи ва танлайдиган киришнинг хусусиятларини тасвирлаш учун мўлжалланган жадвал. Тизим объектига устун, субъектига эса сатр мос келадиган матрицани ўзида акс этиради. Матрицанинг устун ва сатрлари кесишган жойда субъектнинг объектдан эркин фойдаланиш хукуки кўрсатилади.

2. Субъектларнинг ахборот ресурсларидан эркин фойдаланиш қоидаларини акс эттирадиган жадвал.

3. Жадвал кўринишида такдим этилган маълумотларнинг тизимли структураси. Жадвалнинг устунлари тизимда мавжуд бўлган барча ресурсларнинг идентификаторлари билан, сатрлар эса тизимда қайд этилган барча фойдаланувчиларнинг идентификаторлари билан белгиланган. Жадвал ҳар бир устунининг ҳар бир сатр билан кесишиш жойида тизим маъмури томонидан берилган объектдан эркин фойдаланиш турининг муайян фойдаланувчига рухсат этилган махсус кўрсаткичи қўйилади.



## М

### **Матрица полномочий**

**uz** - ваколатлар матрицаси  
**en** - privilege matrix

Таблица, элементы которой определяют права (полномочия, привилегии) определенного объекта относительно защищаемых данных.

### **Мероприятие по защите информации**

**uz** - ахборотни муҳофаза қилиш бўйича тадбир  
**en** - information protective measures

Элементлари муайян объектнинг муҳофаза қилинадиган маълумотларга нисбатан ҳуқуқларини (ваколатларини, имтиёзларини) белгилайдиган жадвал.

Совокупность действий, направленных на разработку и/или практическое применение способов и средств защиты информации.

### **Меры защиты информации организационные**

**uz** - ахборотни муҳофаза қилишнинг ташкилий чора-тадбирлари  
**en** - organizational information protective measures

Ахборотни муҳофаза қилиш усуллари ва воситаларини ишлаб чиқиш ва ёки амалий қўллашга йўналтирилган ҳаракатлар жами.

Меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации.

Маълумотларни қайта ишлаш тизимининг ишлаш жараёнини, тизим ресурсларидан фойдаланишни, персонал фаолиятини, шунингдек, фойдаланувчиларнинг тизим билан ўзаро ҳамкорлик тартибини, тизимда айланувчи ахборот хавфсизлигига таҳдидларни амалга ошириш қийин бўладиган ёки бундай имконият бартараф этиладиган тарзда тартибга соладиган чора-тадбирлар.

## М

### **Меры защиты информации правовые**

**uz** - ахборотни муҳофаза қилишнинг ҳуқуқий чора-тадбирлари

**en** - legal information protective measures

Действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.

Мамлакатда амал қилувчи ахборот билан ишлаш қоидаларини ва уларнинг бузилиши учун жавобгарликни, шу билан ундан ноқонуний фойдаланишга тўсқинлик қиладиган ва потенциал бузғунчиларни тўхтатиб турувчи омил ҳисобланадиган, қонунлар фармойишлар ва бошқа норматив актлар.

### **Меры защиты информации технические**

**uz** - ахборотни муҳофаза қилишнинг техник чора-тадбирлари

**en** - technical information protective measures

Различные электронные устройства и специальные программы, входящие в состав автоматизированной системы, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

Автоматлаштирилган тизим таркибига кирувчи (мустақил ёки бошқа воситалар билан биргаликда), ахборотни муҳофаза қилиш (фойдаланувчиларни идентификациялаш ва аутентификация қилиш, ресурслардан эркин фойдаланишни чеклаш, ҳодисаларни қайд қилиш, ахборотни криптографик ёпиш ва б.к.) функцияларини бажарувчи турли электрон қурилмалар ва махсус дастурлар.

## М

### **Меры защиты информации физические**

**uz** - ахборотни муҳофаза қилишнинг жисмоний чора-тадбирлари  
**en** - physical information protective measures

Разного рода механические, электро- или электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам автоматизированной системы и защищаемой информации, а также технические средства визуального наблюдения, телекоммуникаций и охранной сигнализации.

Автоматлаштирилган тизим ва муҳофаза қилинаётган ахборот компонентларига потенциал бузгунчиларнинг сукулиб кириши ва фойдаланишининг мумкин бўлган йўлларига жисмоний тўсик яратиш учун махсус мўлжалланган ҳар хил турдаги механик, электр ёки электрон-механик қурилмалар ва иншоотлар, шунингдек, телекоммуникация ва қўриқлаш сигнализацияси, визуал кузатиш техник воситалари.

**Метка безопасности**  
**uz** - хавфсизлик белгиси  
**en** - security mark

Маркировка, связанная с ресурсом (которым может быть блок данных), определяющая имя или обозначение атрибутов безопасности данного ресурса.

**Метка грифа**  
**uz** - гриф белгиси  
**en** - security label

Ресурс (маълумотлар блоки бўлиши мумкин) билан боғланган, берилган ресурс хавфсизлик атрибутларининг номи ёки белгиланишини аниқлайдиган маркаш.

Указатель, непосредственно связанный с той информацией, к которой он относится, например, как часть протокола передачи информации.

## М

Ўзи тегишли ахборот билан бевосита, масалан, ахборотни узатиш протоколининг бир қисми сифатида боғлиқ бўлган кўрсаткич.

**Метка идентификационная**

**uz** - идентификацион белги

**en** - identification mark

Подлинная информация (имя автора, программы) в закодированном или зашифрованном виде.

Кодланган ёки шифрланган кўринишдаги ҳақиқий ахборот (муаллиф, дастур номи).

**Метка конфиденциальности**

**uz** - конфиденциаллик белгиси

**en** - confidentiality mark

Элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте.

Объектда мавжуд бўлган ахборотнинг конфиденциаллигини тавсифловчи ахборот элементи.

**Метод аутентификации асимметричный**

**uz** - асимметрик аутентификация қилиш методи

**en** - asymmetric authentication method

Метод аутентификации, при котором не вся информация аутентификации используется обеими сторонами совместно.

Аутентификация қилиш ахборотининг барчасидан иккала томон биргаликда фойдаланмайдиган аутентификация қилиш методи.

**Метод аутентификации симметричный**

**uz** - симметрик аутентификация қилиш методи

**en** - symmetric authentication method

Метод аутентификации, при котором оба объекта совместно используют общую информацию аутентификации.

Иккала объект умумий аутентификация ахборотидан биргаликда фойдаланмайдиган аутентификация қилиш методи.

**Метод записи с частичным разрушением памяти**

Метод, позволяющий создать уникальный рисунок кристалла памяти путем управления процессом ее частичного

## М

**uz** - хотирани қисман  
бузиб ёзиш методи  
**en** - corruptable store  
method

**Метод защиты информации криптографический**  
**uz** - криптографик  
ахборотни муҳофаза  
килиш методи  
**en** - cryptographic in-  
formation protection  
method

**Метод Казиски**  
**uz** - Казиски методи  
**en** - Kazisky's method

**Метод счетчиковый**  
**uz** - ҳисоблагич мето-  
ди  
**en** - counter method

разрушения.

Хотиранинг қисман бузилиш жараёни  
бошқариш йўли билан унинг кристалл  
ноёб шаклини яратишга имкон берувчи  
метод.

Метод защиты информации, основанный  
на принципе ее шифрования и кодирова-  
ния. Криптографический метод может  
быть реализован как программными, так  
и аппаратными средствами.

Шифрлаш ва кодлаш принципига асос-  
ланган ахборотни муҳофаза килиш ме-  
тоди. Криптографик метод ҳам дастурий,  
ҳам аппарат воситалар томонидан амалга  
оширилиши мумкин.

Метод криптоанализа, позволяющий  
вычислять период многоалфавитных  
криптосистем при помощи обнаружения  
одинаковых слов в шифротексте. Если  
период многоалфавитной криптосисте-  
мы становится известным, то криптоана-  
лиз может быть сведен к криптоанализу  
одноалфавитных систем.

Шифр матндаги бир хил сўзларни  
аниқлаш ёрдамида кўп алифболи крип-  
тотизим даврини ҳисоблаш имконини  
берувчи криптотахлил методи. Агар кўп  
алифболи криптотизим даври маълум  
бўлса, криптотахлил бир алифболи ти-  
зимлар криптотахлилига келтирилади.

Режим использования блочного шифра,  
похожий на режим OFB, но на вход ре-  
гистра подается не результат шифрова-  
ния, а некий счетчик, состояние которо-

## М

го увеличивается на константу, обычно единицу.

OFB режимига ўхшаш, блокли шифрдан фойдаланиш режими, регистр киришига шифрлаш натижаси эмас, ҳолати константага, одатда, бирга кўпаядиган хисоблагич узатилади.

### **Механизм информационной безопасности сети телекоммуникаций общего пользования**

**uz** - умум фойдаланишдаги телекоммуникациялар тармоғининг ахборот хавфсизлиги механизми  
**en** - public switched telecommunications network information security mechanism

Аппаратно-программные и организационные средства системы обеспечения информационной безопасности сети телекоммуникаций общего пользования, 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: предотвращение воздействия нарушения, обнаружение последствий, причиненных злоумышленником, восстановление (ликвидация) этих последствий.

*Примечание: К механизмам информационной безопасности сети телекоммуникаций общего пользования при защите процесса передачи сообщений в сети относятся: механизм контроля доступа, механизм аутентификации сообщений, механизм обменной аутентификации.*

Тармокнинг белгиланган ахборот хавфсизлиги сиёсатига мувофиқ, бир-бирини тўлдирувчи учта – бузиш кўрсатадиган таъсирнинг олдини олиш, жинояткор томонидан етказилган оқибатларни аниқлаш, бу оқибатларни тиклаш (баргараф қилиш) каби, муҳофаза қилиш классининг бирига мувофиқ, тармокни ахборот хавфсизлигига бўладиган таҳдидлардан

## М

муҳофаза қилишнинг битта ёки бир нечта аспектини амалга оширадиган умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавфсизлигини таъминлаш тизимининг аппарат-дастурий ва ташкилий воситалари.

*Изоҳ: Тармоқда хабарлар узатиш жараёнини муҳофаза қилишда умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавфсизлиги механизмларига эркин фойдаланишни назорат қилиш механизми, хабарларни аутентификация қилиш механизми, алмашув аутентификация механизми кирди.*

### **Механизм контроля доступа**

**uz** - фойдалана олиш-ни назорат қилиш механизми

**en** - access control mechanism

Оборудование или программное обеспечение, процедуры системы, процедуры администратора и их различные комбинации, которые обнаруживают, предотвращают несанкционированный доступ и разрешают законный в автоматизированных системах.

Рухсат этилмаган тарзда фойдалана олишни аниқлайдиган, бартараф қиладиган ва автоматлаштирилган тизимларда қонуний фойдаланишга рухсат берадиган ускуна ёки дастурий таъминот, тизим процедураси, маъмур процедураси ва уларнинг турли хил комбинациялари.

### **Микроб**

**uz** - микроб

**en** - microbe

Программа, которая способна рассылаться самостоятельно по электронной почте всем адресатам каждого списка доставки.

Электрон почта орқали ҳар бир элтиб бериш рўйхатидаги адресатларга мустақил тарзда тарқалиш қобилиятига эга бўлган дастур.

### **Минимум привиле-**

1. Наделение субъектов только теми

## М

гий

uz - имтиёзлар минимуми

en - least privilege

правами на доступ, которые им необходимы для выполнения конкретных задач. 2. Один из основополагающих принципов организации системы защиты, гласящий, что каждый субъект должен иметь минимально возможный набор привилегий, необходимый для решения поставленных перед ним задач.

*Примечание: Следование этому принципу предохраняет от нарушений, возможных в результате злого умысла, ошибки или несанкционированного использования привилегий.*

1. Субъектларга уларнинг аниқ вазифаларни бажаришлари учун зарур бўлган эркин фойдаланиш ҳуқуқларини бериш.

2. Ҳар бир субъект ўз олдига қўйган вазифаларни ҳал қилиш учун зарур имтиёзларнинг минимал даражада мумкин бўлган тўпламига эга бўлиши керак деб ҳисобловчи муҳофаза тизимини ташкил қилишнинг энг муҳим принципларидан бири.

*Изоҳ: Бу принципга риоя қилиш ёвуз ният, хато ёки имтиёзлардан руҳсат этилмаган тарзда фойдалана оlish натижасида содир бўлиши мумкин бўлган бузилишлардан сақлайди.*

**Модель Белла-Лападула**

uz - Белла-Лападула модели

en - Bella-Lapadula model

Формальная модель описания политики безопасности с использованием теории автоматов, и описывающая множество правил управления доступом. В этой модели компоненты системы делятся на объекты и субъекты. Вводится понятие безопасного состояния и доказывается, что если каждый переход сохраняет безопасное состояние (то есть переводит систему из безопасного состояния в другое безопасное состояние), то согласно принципу индукции, система является безопасной.



## М

Автоматлар назариясидан фойдаланиб, хавфсизлик сиёсатини тавсифлашнинг формал модели ва эркин фойдаланишни бошқаришнинг кўплаб коидаларини тавсифловчи формал модель. Бу моделда тизим компонентлари объектлар ва субъектларга бўлинади. Хавфсизлик ҳолати тушунчаси киритилади, ҳар бир ўтиш хавфсизлик ҳолатини саклаб қолса (яъни тизимни хавфсиз ҳолатдан бошқа хавфсиз ҳолатга ўтказди), индукция принципига мувофиқ тизим хавфсиз ҳисобланиши исбот қилинади.

### Модель данных иерархическая

**uz** - иерархик маълумотлар модели  
**en** - hierarchical data model

Модель данных для представления данных иерархической структуры.

Иерархик структура маълумотларини тақдим этиш учун яратиладиган маълумотлар модели.

### Модель защиты

**uz** - муҳофаза қилиш модели  
**en** - protection model

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

Дастурий-техник воситалар комплекси ва ёки руҳсат этилмаган фойдалана олишдан муҳофаза қилиш ташкилий чора-тадбирларининг мавҳум (формаллаштирилган ёки формаллаштирилмаган) тавсифи.

### Модель информационных угроз (техническими средствами)

**uz** - ахборот таҳдидлари (техник воситалар билан амалга оши-

Формализованное описание технических каналов утечки, сведения о методах и средствах реализации информационных угроз.

Ахборот чиқиб кетадиган техник канал-

## М

риладиган) модели  
**en** - information treats  
model (by technical  
facilities)

**Модель концепту-  
альная**

**uz** - концептуал модел  
**en** - conceptural model

**Модель нарушителя  
правил доступа**

**uz** - фойдалана олиш  
қоида-ларини бузув-  
чининг модели  
**en** - access rules viola-  
tor's model

**Модель политики  
безопасности фор-  
мальная**

**uz** - формал хавфсиз-  
лик сиёсати модели  
**en** - formal security  
policy model

ларнинг формаллаштирилган тавсифи,  
ахборот таҳдидларини амалга ошириш-  
нинг методлари ҳамда воситалари  
тўғрисидаги маълумотлар.

Формальное представление проблемной  
области на понятийном уровне.

Муаммоли соҳанинг тушунча даражаси-  
да формал тақдим этилиши.

Абстрактное (формализованное или не-  
формализованное) описание нарушителя  
правил доступа к информационному ре-  
сурсу.

*Примечание: Примерами моделей нарушите-  
ля правил доступа являются такие програм-  
мы как троянский конь, логическая бомба,  
компьютерный вирус и другие.*

Ахборот ресурслардан эркин фойдаланиш  
қоидаларини бузувчининг абстракт  
(формаллаштирилган ёки формаллашти-  
рилмаган) тавсифи.

*Изоҳ: Троя оти, мантиқий бомба, компь-  
тер вируси ва бошқалар эркин фойдаланиш  
қоидаларини бузувчининг моделлариға мисол  
бўлади.*

Математически строгое описание поли-  
тики безопасности, подразумевающее  
описание начального состояния систе-  
мы, способы перехода системы из одно-  
го состояния в другое, а также определе-  
ние безопасного состояния. Примером  
формальной модели является модель  
Белла-Лападула.

Тизим бошланғич ҳолати тавсифини, ти-  
зимнинг бир ҳолатдан иккинчи ҳолатға  
ўтиш усулларини, шунингдек, хавфсиз

## М

ҳолат аниқланишини назарда тутувчи хавфсизлик сиёсатининг катъий математик тавсифи. Белла-Лападула модели формал моделга мисол бўлади.

**Модификация**  
**uz** - ўзгартириш  
**en** - modification

Неавторизованное изменение данных в базах данных или в файлах автоматизированной системы, изменение алгоритмов используемых программ с целью выполнения некоторой дополнительной несанкционированной обработки.

Автоматлаштирилган тизим файлларидаги ёки маълумотлар базасидаги маълумотларнинг муаллифлаштирилмаган тарзда ўзгартирилиши, фойдаланиладиган дастурлар алгоритмларининг, баъзи бир қўшимча, рухсат этилмаган тарзда қайта ишлашни бажариш мақсадида, ўзгартирилиши.

**Модификация информации**  
**uz** - ахборотни ўзгартириш  
**en** - information modification

Несанкционированное изменение содержания или объема информации на ее носителях при обработке техническими средствами.

Техник воситалар билан қайта ишлашда ташувчилардаги ахборотнинг мазмуни ёки ҳажмини рухсат этилмаган тарзда ўзгартириш.

**Модуль защиты интеллектуальный**  
**uz** - интеллектуал муҳофаза қилиш модули  
**en** - smart protection card

Аппаратно-программная схема защиты программного обеспечения, характеризующаяся высоким уровнем защищенности и использующая процессор.

Дастурий таъминотни муҳофаза қилишнинг, юқори даражада муҳофазаланганлик билан тавсифланувчи ҳамда процессордан фойдаланувчи аппарат-дастурий схемаси.

## М

**Модуль идентификации абонента (SIM-карта)**

**uz** - абонентни идентификациялаш модули (SIM-карта)

**en** - subscriber identification module, SIM

Пластиковая карточка с микрочипом, в памяти которой хранятся идентификационный номер, ключ аутентификации и криптографический алгоритм, необходимый для реализации процедуры аутентификации.

Микрочипли пластик карточка, унинг хотирасида аутентификация процедурасини амалга ошириш учун зарур бўлган идентификацион рақам, аутентификация калити ва криптографик алгоритм сақланади.

**Модуль идентификационный сменный**

**uz** - идентификацион алмаштириладиган модуль

**en** - removable user identity module, R-UIM

Разновидность смарт-карты, которая может быть легко удалена из одного абонентского аппарата и вставлена в другой.

Бир абонент аппаратидан осон олинадиган ва бошқасига қўйиладиган смарт-картанинг бир тури.

**Модуль услуг пользователя идентификационный**

**uz** - идентификацион фойдаланувчи хизматлари модули

**en** - user services identity module, USIM

Универсальная смарт-карта в сети UMTS, являющаяся аналогом SIM-карты в GSM, но с более широким набором услуг.

GSM даги SIM-картага ўхшаш, лекин хизматларнинг кенг тўпламига эга бўлган, UMTS тармогидаги универсал смарт-карта.

**Монитор (программа)**

**uz** - монитор (дастур)

**en** - monitor (software)

Резидентно находящаяся в оперативной памяти утилита, которая позволяет выявлять «подозрительные» действия пользовательских программ: изменение и переименование выполняемых программ (СОМ- и ЕХЕ-файлов), запись на диск по абсолютному адресу, форматирование диска и т.д.

## М

Оператив хотирада резидентлик билан жойлашган утилита. Фойдаланувчилар дастурларининг «шубҳали» ҳаракатларини аниқлаш: бажариладиган дастурларнинг (СОМ ва ЕХЕ файлларнинг) ўзгартирилишини ёки қайта номланишини, абсолют адрес бўйича дискка ёзиш, дискни форматлаш ва ҳ.к. аниқлаш имконини беради.

### **Монитор ссылок**

**uz** - ҳаволалар монитори

**en** - reference monitor concept

Концепция контроля доступа, базирующаяся на понятии абстрактной машины, разделяющей все попытки доступа субъектов к объектам. Находит практическую реализацию в виде ядра безопасности.

Субъектларнинг объектлардан эркин фойдаланиш учун бўлган барча уринишларини ажратувчи абстракт машина тупунчасига асосланувчи эркин фойдаланишни назорат қилиш концепцияси. Ядро ҳавфсизлиги кўринишида амалга оширилади.

### **Мошенничество**

**uz** - фирибгарлик

**en** - fraud

Любые незаконные действия, связанные с использованием ресурсов мобильной сети связи без надлежащей оплаты за эфирное время, например путем предоставления ложных сведений.

Эфир вақти учун тегишли тўловларсиз, масалан, ёлғон маълумотларни тақдим этиш йўли билан мобил алоқанинг тармоғи ресурсларидан фойдаланиш билан боғлиқ ҳар қандай ноқонуний ҳаракат.

### **Мошенничество**

**компьютерное**

**uz** - компьютер фирибгарлиги

Мошенничество, совершенное с помощью или при непосредственном использовании системы обработки данных или компьютерной сети.

## М

en - computer fraud

Маълумотларни қайта ишлаш тизими ёки компьютер тармоғи ёрдамида ёки ундан бевосита фойдаланган ҳолда содир этилган фирибгарлик.

**Мошенничество  
процедурное**

uz - процедура фирибгарлиги

en - procedural fraud

Незаконное использование роуминга и других сетевых процедур (например, биллинга) с целью уменьшения оплаты услуг связи.

**Мошенничество с  
карточками предоплаты**

uz - олдиндан тўлов карточкалари билан боғлиқ фирибгарлик

en - prepaid fraud

Любые действия, связанные с незаконными способами пополнения счета с помощью предоплаченных карточек.

Олдиндан тўланган карточкалар ёрдамида ҳисобни тўлдиришнинг ноқонуний усуллари билан боғлиқ ҳар қандай ҳаракат.

**Мошенничество с  
контрактами**

uz - контрактлар билан боғлиқ фирибгарлик

en - subscription fraud

Преднамеренное указание ложных сведений при заключении контракта с оператором сети мобильной связи.

Мобил алоқа тармоғи оператори билан контракт тузишда ёлғон маълумотларни атайлаб кўрсатиш.

**Мошенничество с  
украденным телефоном**

uz - ўғирланган телефон билан боғлиқ фирибгарлик

en - stolen phone fraud

Несанкционированное использование украденного или потерянного сотового телефона обычно до тех пор, пока владелец не заявит о его пропаже, а оператор не заблокирует номер.

Ўғирланган ёки йўқотилган сотали телефондан, эгаси уни йўқотгани тўғрисида хабар бергунгача, оператор эса рақамни

## М

блокировка қилгунгача рухсат этилмаган тарзда фойдаланиш.

**Мошенничество, основанное на умении общения**

**uz** - мулоқот қила олишга асосланган фирибгарлик  
**en** - fraud based on communication ability

Искусство обмана пользователей или администраторов сетей путем выведывания у них сведений, необходимых для незаконного доступа в сеть; обычно осуществляется путем обращения к ним от имени авторизованного пользователя.

Фойдаланувчилар ёки тармоқ маъмурларини, улардан тармоқдан ноқонуний фойдалана олиш учун зарур бўлган маълумотларни билиб олиш йўли билан алдаш маҳорати; одатда, муаллифлаштирилган фойдаланувчи номидан уларга мурожаат қилиш орқали амалга оширилади.

## Н

**Наблюдатель**

**uz** - кузатувчи  
**en** - lurker

1. Человек, занимающийся тайным просмотром.
2. Лицо, читающее письма на электронной доске объявлений, но не принимающее никакого участия в их обсуждениях и не отправляющее туда свои письма.

1. Яширин кўриб чиқиш билан шуғулланувчи одам.
2. Электрон эълонлар тахтасидаги хатларни ўқувчи, лекин уларнинг муҳокамасида иштирок этмайдиган ва у ерга ўзининг хатларини юбормайдиган шахс.

**Наблюдение**

**uz** - кузатиш  
**en** - lurking

Чтение группы новостей без участия в их обсуждении.

Янгиликлар туркумини, уларнинг муҳокамасида иштирок этмасдан, ўқиш.

## Н

### **Надежность информационная**

**uz** - ахборотнинг  
ишончлилиги  
**en** - information  
reliability

1. Способность алгоритма или программы правильно выполнять свои функции при различных ошибках в исходных данных.
2. Способность информационной системы обеспечивать целостность хранящихся в ней данных.

### **Надежность сети**

**uz** - тармоқнинг  
ишончлилиги  
**en** - network  
reliability

1. Алгоритм ёки дастурнинг, дастлабки маълумотларда турли хатолар бўлганда, ўз функцияларини тўғри бажариш қобилияти.
2. Ахборот тизимининг унда сақланадиган маълумотлар яхлитлигини таъминлаш қобилияти.

Свойство сети сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях использования и технического обслуживания.

Тармоқнинг берилган режимларда ва фойдаланиш ҳамда техник хизмат кўрсатиш шароитларида талаб қилинадиган функцияларни бажариш қобилиятини тавсифловчи барча параметрлар қийматларини белгиланган чегарада вақт бўйича сақлаш хусусияти.

### **Нападение**

**uz** - хужум  
**en** - hijacking

Попытка злоумышленника разрушить систему безопасности сервера путем передачи серии сетевых пакетов, фальсифицирующих действия законного клиента.

Жинояткорнинг сервернинг хавфсизлик тизимини қонуний мижозларнинг ҳаракатини сохталаштирувчи тармоқ пакетларининг туркуминини узатиш йўли билан бузишга уриниши.

### **Нарушение защи-**

Обход системы компьютерной безопасно-



## Н

**ты**

**uz** - мухофаза

қилишнинг бузи-  
лиши

**en** - security breach

сти или вывод из строя какого-либо ее элемента, результатом которого может быть проникновение в систему обработки данных.

Компьютер хавфсизлиги тизимини четлаб ўтиш ёки унинг бирор-бир элементини ишдан чиқариш, натижада маълумотларни қайта ишлаш тизимига кириб олиш мумкин бўлади.

**Нарушение цело-  
стности**

**uz** - яхлитликнинг  
бузилиши

**en** - integrity  
violation

Искажение содержимого записей файла или базы данных, которое происходит вследствие машинных сбоев, программных ошибок, а также ошибочных действий пользователей.

Файл ёзувлари ёки маълумотлар базаси таркибидагиларнинг машина билан боғлиқ узилишлар, дастурдаги хатолар, шунингдек, фойдаланувчиларнинг нотўғри ҳаракатлари оқибатида юз берадиган ўзгариши.

**Нарушитель**

**uz** - бузғунчи

**en** - intruder

Лицо (субъект), которое предприняло (пыталось предпринять) попытку несанкционированного доступа к ресурсам системы (попытку выполнения запрещенных ему действий с данным ресурсом) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или с целью самоутверждения и т.п.) и использовавшее для этого различные возможности, методы и средства.

Тизим ресурсларидан рухсат этилмаган тарзда фойдалана олишга (бу ресурс билан ишлашда унинг учун таъқиқланган ҳаракатларни бажаришга уриниш) хато, билмаслик оқибатида ёки ёвуз ниятда (ўз манфаатлари йўлида) ёки шунчаки (ўйин ёки ўзини на-

## Н

- моён қилиш мақсадида) уринган (уриниб кўрган) ва бунинг учун турли хил имкониятлар, методлар ва воситалардан фойдаланган шахс (субъект).
- Нарушитель правил доступа**  
uz - эркин фойдаланиш қоидаларини бузувчи  
en - access rule breaker
- Лицо, осуществляющее несанкционированный доступ к информационному ресурсу с использованием штатных технических средств.**  
Штат техник воситалар ёрдамида ахборот ресурслардан рўхсат этилмаган тарзда эркин фойдаланадиган шахс.
- Недоверие взаимное**  
uz - ўзаро ишончсизлик  
en - mutual distrust
- Отношения между взаимодействующими логическими объектами, когда ни один из них не полагается на безошибочность или надежность выполнения функций другим логическим объектом относительно некоторых свойств.**  
Биргаликда ишлайдиган мантиқий объектлар ўртасидаги муносабат, бунда улардан бирортаси ҳам бошқа мантиқий объект томонидан баъзи хусусиятларга нисбатан функцияларнинг бажарилишини хатосиз ёки ишончли деб ҳисобламайди.
- Незащищенность**  
uz - муҳофаза қилинмаганлик  
en - insecurity
- Возможность использования конкретной уязвимости системы обработки данных при проведении конкретной атаки.**  
Муайян хужум амалга оширилганда маълумотларни қайта ишлаш тизимининг муайян заифлигидан фойдаланиш имконияти.
- Неотказуемость**  
uz - рад этолмаслик  
en - non-repudiation
- Процедура обмена электронными документами с гарантированной доставкой сообщений. В результате такой процедуры отправитель не может отрицать факт передачи, а получатель то, что сообщение не было дос-**

## Н

тавлено в срок.

Хабарларни кафолатли етказиб бериш билан электрон хужжатларни алмашиш процедураси. Бундай процедура натижасида жўнатувчи узатиш фактини, олувчи эса хабар муддатида етказилмаганлигини рад этолмайди.

### Непризнание участия

uz - иштирокни тан олмаслик  
en - repudiation

1. Отрицание одним из логических объектов, участвующих в обмене данными, полного или частичного своего участия в этом обмене. *Примечание: В описании методов и механизмов часто используется термин «неотказуемость», который подразумевает, что ни один из взаимодействующих логических объектов не может отрицать свое участие в обмене данными.*

2. Отрицание одной из сторон участия в информационном обмене, а также факта получения сообщений в электронном виде.

1. Маълумотлар алмашинишда иштирок этадиган мантикий объектлардан бирининг бу алмашинишда ўзининг иштирокини тўлиқ ёки қисман тан олмаслиги.

*Изоҳ: Метод ва механизмларнинг баёнида, кўнчилиқ ҳолларда, биргаликда ишлайдиган мантикий объектлардан биронтаси ҳам маълумотлар алмашинишдаги ўзининг иштирокини рад эта олмаслиги назарда тутилган «рад этолмаслик» атамасидан фойдаланилади.*

2. Томонлардан бирининг ахборот алмашинишда ўз иштирокини, шунингдек, хабарларни электрон кўринишда олганлик фактини рад этиши.

### Нестойкость

uz - бардошсизлик  
en - nonpersistence

Возможность несанкционированного ознакомления криптоаналитиками с алгоритмом при генерации, распространении и хранении ключей.

## Н

Калитларни генерациялаш, тарқатиш ва сақлашда криптоаналитикларнинг алгоритм билан рухсат этилмаган тарзда танишиш имконияти.

**Нечувствительность к отказам**

**uz** - ишламай

қолишларга

таъсирчан

бўлмаслик

**en** - fault tolerance

Свойство программы или системы сохранять правильность функционирования при наличии ошибок или отказов.

**Номер идентификационный персональный**

**uz** - шахсий иден-

тификация раками

**en** - personal identification number, PIN

Дастур ёки тизимнинг хатолар мавжуд бўлган ёки ишламай қолишлар шароитида тўғри ишлашини сақлаб қолиш хусусияти.

1. Уникальный код, хранимый на смарт-карте и используемый для аутентификации личности пользователя.

2. Персональный код некоторого лица, обеспечивающий ему возможность входа в систему с управляемым доступом.

3. Вид пароля, который должен быть указан терминалу вместе, например, с магнитной картой для получения доступа к системе.

1. Смарт-картада сақланадиган ва фойдаланувчининг шахсини аутентификация қилиш учун ишлатиладиган уникал код.

2. Қандайдир шахснинг унга бошқариладиган тизимга кириш имконини берадиган шахсий коди.

3. Тизимга киришга рухсат олиш учун магнит карта билан бирга терминалга кўрсатиладиган пароль тури.

**Номер порядковый**

**uz** - тартиб раками

**en** - sequence number, SQN

Текущий номер пакета или сообщения, с помощью которого приемник всегда информирован о порядке поступления данных; позволяет обнаружить подмену данных в процессе передачи.

Пакет ёки хабарнинг жорий раками, унинг

## Н

ёрдамида қабул қилгич ҳар доим маълумотларнинг келиб тушиш тартиби тўғрисида хабардор бўлади; узатиш жараёнида маълумотлар алмаштирилганлигини аниқлашга имкон беради.

### Норма безопасности

uz - хавфсизлик нормаси  
en - safety standard

Количественное значение критерия безопасности информации, устанавливаемое в зависимости от категории безопасности.

Хавфсизлик категориясига боғлиқ равишда ўрна-тиладиган, ахборот хавфсизлиги критерийининг миқдор қиймати.

### Нормы эффективности защиты информации

uz - ахборотни муҳофаза қилиш самарадорлигининг нормалари  
en - information security efficiency rates

Значения показателей эффективности защиты информации, установленные нормативными документами.

Норматив ҳужжатлар билан белгиланган ахборотни муҳофаза қилиш самарадорлиги кўрсаткичларининг қийматлари.

### Носители информации

uz - ахборот ташувчилар  
en - data carrier

Материальные объекты (в т.ч. и люди), предназначенные для хранения, обработки и передачи информации.

Ахборотни сақлаш, қайта ишлаш ва узатиш учун мўлжалланган моддий объектлар (шу жумладан, одамлар).

### Носители сведений, являющиеся государственными секретами

uz - давлат сир ҳисобланадиган маълумотларни ташувчилар

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.

Давлат сирларини ташкил қиладиган маъ-

## Н

**en** - bearers of state secrets

лумотлар хотира, символлар, образлар, сигналлар, техник ечимлар ва жараёнлар кўринишида акс этадиган жисмоний шахслар, моддий объектлар, шу жумладан, физик майдонлар.

**Нотаризация**  
**uz** - нотариаллаштириш  
**en** - notarization

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

Маълумотларни учинчи ишончли томондан қайд этилиши, бу эса кейинчалик уларнинг ичидаги жўнатувчи, вақт ва олувчи каби тавсифларининг тасдиқланишини таъминлайди.

## О

**Обеспечение программного безопасное**  
**uz** - хавфсиз дастурий таъминот  
**en** - security software

Общечеловеческие и прикладные программы и средства, осуществляющие безопасную обработку данных в системе или сети и безопасно использующие ресурсы системы.

Тизим ёки тармоқда маълумотларнинг хавфсиз қайта ишланишини амалга оширувчи, тизим ресурсларидан хавфсиз фойдаланувчи умумий мақсадлардаги ҳамда амалий дастур ва воситалар.

**Обеспечение программного достоверное**  
**uz** - ишончли дастурий таъминот  
**en** - trusted software

Программное обеспечение, входящее в достоверную вычислительную базу (ДВБ).

Ишончли ҳисоблаш базаси (ИХБ)га кирувчи дастурий таъминот.

**Область блокирования**  
**uz** - блокировкалаш соҳаси

Часть базы данных (запись, область, файл), открытая для монопольной обработки одной программой и недоступная до момента закрытия другим программам.

## О

en - locking unit

Маълумотлар базасининг битта дастур томонидан монополь (якка) қайта ишлаш учун очик бўлган, ёпилиш пайтигача бошқа дастурлар фойдалана олмайдиган қисми (ёзув, соҳа, файл).

**Область предметная**

uz - предмет соҳа

en - universe of discourse

Совокупность всех объектов, которые были, есть или будут в выбранной части реального или условного мира представлять интерес с точки зрения их описания.

Реал ёки шартли оламнинг танланган қисмида уларни тавсифлаш нуқтаи назаридан қизиқиш уйғотадиган, илгари бўлган, ҳозирда мавжуд ва мавжуд бўладиган барча объектларнинг жами.

**Обманывать**

uz - алдамоқ

en - to spoof

Выполнять действия, направленные на введение в заблуждение пользователя, наблюдателя (например, оператора перехвата сообщений) или ресурса.

Фойдаланувчини, кузатувчини (масалан, хабарларни тутиб олувчи операторни) ёки ресурсни чалғитишга йўналтирилган ҳаракатларни бажариш.

**Обмен данными**

uz - маълумотлар

алмашинуви

en - data

communication

Процедура приема и передачи данных, включая кодирование, декодирование буферизацию и проверку.

Маълумотларни қабул қилиш ва узатиш процедураси, жумладан, кодлаш, декодлаш, буферлаш ва текшириш.

**Обмен данными безопасности**

uz - хавфсизлик

маълумотлари алмашинуви

en - security

exchange

Передача или последовательность передач данных управления-протокола-приложения между открытыми системами, являющихся частью работы одного или нескольких механизмов обеспечения безопасности.

Очик тизимлар ўртасида бошқариш-

## О

протокол-илова маълумотларини узатиш ёки узатишлар кетма-кетлиги. Бир ёки бир нечта хавфсизликни таъминлаш механизмларининг иши ҳисобланади.

### **Обмен ключами**

**uz** - калитлар ал-  
машинуви

**en** - key exchange

Обмен между объектами открытыми ключами, которые должны использоваться для кодирования связи между этими объектами.

Объектлар ўртасида бу объектлар орасида боғлианишни кодлаш учун фойдаланилиши керак бўлган очик калитларни алмашиниш.

### **Обмен при установлении подлинности**

**uz** - ҳақиқийликни  
аниқлашдаги ал-  
машиш

**en** - authentication  
exchange

Механизм, предназначенный для установления подлинности какого-либо объекта посредством обмена информацией.

Ахборот алмашуви ёрдамида қандайдир объектнинг ҳақиқийлигини аниқлаш учун мўлжалланган механизм.

### **Обнаружение атак**

**uz** - хужумларни  
аниқлаш

**en** - attack detection

Механизм, используемый для обнаружения атак на объекты системы.

Тизим объектларига бўладиган хужумларни аниқлаш учун қўлланиладиган механизм.

### **Обнаружение манипуляции**

**uz** - манипуляцияни  
аниқлаш

**en** - manipulation  
detection

Процедура, которая используется для обнаружения случайной или умышленной модификации данных.

Маълумотларнинг тасодифан ёки қасдан қилинадиган ўзгартиришларни аниқлаш учун қўлланиладиган процедура.

### **Обновление ключей быстрое**

**uz** - калитларни тез  
янгилаш

**en** - key freshness

Метод защиты от вскрытия ключевой информации, при котором в каждом новом сеансе связи ключи обновляются, при этом ни один из них повторно не используется.



## О

Калитли ахборотни очишдан муҳофаза қилиш методи, унга кўра, ҳар бир янги алоқа сеансида калитлар янгиланади, бунда калитларнинг ҳеч қайсиси такроран ишлатилмайди.

### **Оборудование криптографическое**

**uz** - криптографик ускуна  
**en** - cryptographic equipment

Аппаратные, программно-аппаратные, программные комплексы и средства для шифрования, расшифрования, изготовления шифрключей и защиты от несанкционированного доступа, реализующие криптографические алгоритмы и предназначенные для защиты информации при ее передаче, обработке и хранении.

Криптографик алгоритмларни амалга оширувчи, шифрлаш, дастлабки матнга ўгириш, шифр калитларни тайёрлаш, рухсат этилмаган тарзда фойдалана олишдан муҳофаза қилиш ва ахборотни узатиш, қайта ишлаш ва сақлашда муҳофаза қилиш учун мўлжалланган аппарат, дастурий-аппарат, дастурий комплекс ва воситалар.

### **Обработка информации в автоматизированной системе**

**uz** - автоматлаштирилган тизимда ахборотни қайта ишлаш  
**en** - information processing in the automated system

Совокупность операций (сбор, накопление, хранение, преобразование, отображение, выдача и т.п.), осуществляемых над информацией (сведениями, данными) с использованием средств автоматизированной системы.

Автоматлаштирилган тизим воситаларидан фойдаланиб ахборот (маълумотлар) устида амалга ошириладиган операциялар (йиғиш, тўплаш, сақлаш, ўзгартириш, акс эттириш, узатиш ва ш.к.) жами.

### **Образ**

**uz** - образ  
**en** - image

Точная копия совокупности данных (возможно, в другой среде хранения информации), на основе которой может быть восстановлен оригинал данных.

## О

Маълумотлар жамининг аниқ нусхаси (ахборотни сақлашнинг бошқа мухитида), унинг асосида маълумотларнинг оригинали тикланиши мумкин.

### Объект

uz - объект

en - object, unit

1. Логический объект, доступ к которому контролируется.

Например, файл, программа, область оперативной памяти, собранные и хранимые персональные данные.

2. Пассивный компонент системы, хранящий, принимающий или передающий информацию, доступ к которому регламентируется правилами разграничения доступа.

*Примечание: Доступ к объекту подразумевает доступ к содержащейся в нем информации.*

*Примеры объектов: записи, блоки, страницы, сегменты, файлы, директории и программы, а также отдельные биты, байты, слова, поля; различные устройства (терминалы, принтеры, дисководы и т.д.); различные сетевые устройства (отдельные узлы, кабели и т.д.).*

1. Фойдаланилиши назорат қилинадиган мантикий объект.

Масалан, файл, дастур, оператив хотира доираси; йиғилган ва сақланаётган шахсий маълумотлар.

2. Ахборотни сақловчи, қабул қилувчи ёки узатувчи тизимнинг пассив компоненти, ундан фойдалана олиш эркин фойдаланиш-ни чеклаш қоидалари билан тартибга соли-нади.

*Изоҳ: Объектдан фойдалана олишда унда сақлана-ётган ахборотдан эркин фойдаланишни англата-ди. Объектлар: ёзувлар, блоклар, саҳифалар, сег-ментлар, файллар, директориялар ва дастурлар, шунингдек, алоҳида битлар, байтлар, сўзлар, май-донлар; турли қурилмалар (терминаллар, прин-терлар, дисководлар ва Ҳ.К.); турли тармоқ қурилмалари (алоҳида узеллар, кабеллар ва Ҳ.К.).*

## О

### **Объект безопасности**

**uz** - хавфсизлик  
объекти  
**en** - security object

### **Объект вычислительной техники**

**uz** - ҳисоблаш техникаси  
объекти  
**en** - computer  
technology object

Пассивная системная составляющая, к которой применяется политика безопасности.

Хавфсизлик сиёсати қўлланиладиган тизимнинг пассив ташкил этувчиси.

Стационарный или подвижный объект, который представляет собой комплекс средств вычислительной техники, предназначенный для выполнения определенных функций обработки информации.

*Примечание: К объектам вычислительной техники относятся автоматизированные системы (АС), автоматизированные рабочие места (АРМ), информационно-вычислительные центры (ИВЦ) и другие комплексы средств вычислительной техники, а также отдельные средства вычислительной техники, выполняющие самостоятельные функции обработки информации.*

Ўзида ахборотни қайта ишлашнинг муайян функцияларини бажариш учун мўлжалланган ҳисоблаш техникаси воситаларининг комплексини ифодаловчи стационар ёки кўчма объект.

*Изоҳ: Ҳисоблаш техникаси объектларига автоматлаштирилган тизимлар (АТ), автоматлаштирилган иш ўринлари (АИЎ), ахборот ҳисоблаш марказлари (АҲМ) ва ҳисоблаш техникаси воситаларининг бошқа комплекслари, шунингдек, ахборотни қайта ишлашнинг мустақил функцияларини бажарадиган ҳисоблаш техникасининг алоҳида воситалари ҳам қиради.*

### **Объект доступа**

**uz** - фойдалана  
олиш объекти  
**en** - access object

Единица информационного ресурса системы, доступ к которой регламентируется правилами разграничения доступа.

Тизимнинг ахборот ресурси бирлиги, ундан фойдалана олиш эркин фойдаланишни чегаралаш қоидалари билан тартибга солинади.

## О

### **Объект защиты информации**

**uz** - ахборотни муҳофаза қилиш объекти  
**en** - information security object

### **Объект информатики заштитенный**

**uz** - муҳофазаланган информатика объекти  
**en** - protected informatics object

### **Объект информационного обмена**

**uz** - ахборот алмашиниш объекти  
**en** - information exchange object

### **Объект информационной безопасности сети телекоммуникаций общего пользования**

**uz** - умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавф-

Информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

Ахборотни муҳофаза қилиш бўйича қўйилган мақсадга мувофиқ муҳофаза қилиниши зарур бўлган ахборот ёки ахборот ташувчи, ёинки ахборот жараёни.

Объект информатики, соответствующий требованиям стандартов и других нормативных документов по обеспечению безопасности обрабатываемой информации.

Қайта ишланадиган ахборотнинг хавфсизлигини таъминлаш бўйича стандартлар ва бошқа норматив ҳужжатларнинг талабларига мос келадиган информатика объекти.

Пассивная единица информационного обмена. Например, информационный пакет данных, файл, каталог, электронное письмо, пароль, электронная подпись и др.

Ахборот алмашинишнинг пассив бирлиги. Масалан, маълумотларнинг ахборот пакети, файл, каталог, электрон хат, пароль, электрон имзо ва бошқалар.

Объект(ы) сети телекоммуникаций общего пользования, воздействия злоумышленника на который(ые) может привести к реализации угрозы информационной безопасности сети телекоммуникаций общего пользования.

Умумий фойдаланишдаги телекоммуникациялар тармоғи объект(лар)и, жинояткорнинг унга (уларга) бўладиган таъсири уму-

## О

сизлиги объекти  
**en** - public switched  
telecommunications  
network information  
security object

**Объект конечный**  
**uz** - охирги объект  
**en** - terminal object

**Объекты информатики**  
**uz** - информатика  
объектлари  
**en** - information  
science objects

**Объекты режимные**  
**uz** - режимли объектлар  
**en** - secret entities

мий фойдаланишдаги телекоммуникациялар тармоғининг ахборот хавфсизлигига тахдид амалга оширилишига олиб келиши мумкин.

Субъект, который имеет сертификат и использует свой личный ключ не для целей подписи сертификатов, или объект, который является доверенной стороной.

Сертификати бўлган, ўзининг шахсий калитидан сертификатларни имзолаш мақсадларида фойдаланмайдиган субъект ёки ишончли томон ҳисобланадиган объект.

Автоматизированные системы различного назначения, системы телекоммуникаций, отображения и размножения вместе с помещениями, в которых они установлены, а также отдельные технические средства обработки информации и помещения, предназначенные для ведения конфиденциальных переговоров.

Турли мақсадлардаги автоматлаштирилган тизимлар, телекоммуникациялар тасвирлаш, кўпайтириш тизимлари, улар ўрнатилган хоналар билан бирга, шунингдек, ахборотни қайта ишлаш айрим техник воситалари ҳамда конфиденциал музокаралар олиб бериш учун мўлжалланган хоналар.

Организации, технологическое производство которых, отчеты содержат сведения, составляющие государственные секреты.

Технологик ишлаб чиқариши, ҳисоботлари давлат сирини ҳисобланадиган маълумотлари ўз ичига оладиган ташкилотлар.

## О

### **Один звонок**

**uz** - битта кўнғирок  
**en** - wan-giri

Метод мошенничества, при котором сотовый телефон звонит только один раз, а если владелец перезванивает на определившийся телефонный номер, то мошенник через некоторое время высылает ему счет на солидную сумму.

Фирибгарлик методи, бунда сотали телефон факат бир марта жиринглайди, агар унинг эгаси аниқланган телефон ракамига қайта кўнғирок килса, фирибгар маълум вақт ўтгандан сўнг унга катта микдордаги сумага хисоб юборди.

### **Определитель события**

**uz** - ходисани аниқлагич  
**en** - event discriminator

Функция, которая обеспечивает первоначальный анализ события, имеющего отношение к обеспечению безопасности, и вызывает, по мере необходимости, проверку безопасности и/или сигнал тревоги.

Хавфсизликни таъминлашга алоқаси бўлган ходисанинг дастлабки таҳлилини таъминлайдиган ва заруратга қараб, хавфсизлик ваёки тревога сигнали текширилишини келтириб чиқарадиган функция.

### **Орган**

**uz** - орган  
**en** - authority

Объект, ответственный за выдачу сертификатов. Определены два типа органов: орган сертификации, который выдает сертификаты открытых ключей, и орган по присвоению атрибутов, который выдает сертификаты атрибутов.

Сертификатлар берилиши юзасидан жавобгар объект. Органларнинг икки типи: очик калитлар сертификатларини берадиган сертификатлаш органи ҳамда атрибутлар сертификатларини берадиган атрибутлар органи белгиланган.

### **Орган безопасно-**

1. Объект, ответственный за определение,

## О

**сти**  
**uz** - хавфсизлик  
органи  
**en** - security  
authority

реализацию и выполнение политики безопасности.

2. Объект, ответственный за управление политикой безопасности в домене безопасности.

3. Администратор, ответственный за реализацию политики безопасности.

1. Хавфсизлик сиёсатининг белгиланиши, амалга оширилиши ва бажарилиши юзасидан жавобгар объект.

2. Хавфсизлик доменида хавфсизлик сиёсатини бошқариш юзасидан жавобгар объект.

3. Хавфсизлик сиёсати амалга оширилиши юзасидан жавобгар маъмур.

**Орган по присвоению атрибутов**  
**uz** - атрибутлар берувчи орган  
**en** - attribute authority

1. Орган, который назначает полномочия путем выдачи сертификатов атрибутов.

2. Объект, которому один или несколько объектов доверяют создание и подпись сертификатов атрибутов.

1. Атрибутлар сертификатларини бериш йўли билан ваколатлар белгиловчи орган.

2. Битта ёки бир нечта объект атрибутлар сертификатларини тузиш ва имзоланишини ишониб топширадиган объект.

**Орган по сертификации в области защиты информации**  
**uz** - ахборотни муҳофаза қилиш соҳасида сертификатлаш органи  
**en** - certification authority in field of information security

Орган, проводящий сертификацию защищенных изделий, технических средств и способов защиты информации на соответствие конкретному стандарту или другому документу.

Муҳофазаланган буюмлар, ахборотни муҳофаза қилиш техник воситалари ва усуллари ринг маълум бир стандартга ёки бошқа хужжатга мувофиқлик сертификациясини ўтказувчи орган.

## О

### **Орган регистра- ции**

**uz** - рўйхатга олиш  
органи

**en** - registration  
authority, RA

1. Какой-либо объект, отвечающий за идентификацию и аутентификацию субъектов сертификатов, но не являющийся органом сертификации и органом по присвоению атрибутов.

2. Орган, которому предоставлено право и доверено предоставлять услугу регистрации.

1. Сертификатлар субъектларини идентификациялаш ва аутентификация қилиш юзасидан жавобгар, бироқ сертификатлаш органи ҳам, атрибутлар бериш органи ҳам бўлмаган қандайдир объект.

2. Рўйхатга олиш хизматини тақдим этиш ҳуқуқи берилган ва ишониб топширилган орган.

### **Орган режимно- секретный (PCO)**

**uz** – махфий режим  
органи (MPO)

**en** - regime and se-  
cret authority

Самостоятельное структурное подразделение, разрабатывающее и осуществляющее мероприятия по обеспечению режима секретности и проводящее постоянный контроль за его соблюдением в организациях, где ведутся секретные работы.

Махфийлик режимини таъминлаш бўйича тадбирларни ишлаб чиқувчи ва амалга оширувчи ҳамда махфий ишлар юритиладиган ташкилотларда унга риоя қилинишини мунтазам текшириб турадиган мустақил ташкилий бўлинма

### **Орган сертифика- ции**

**uz** - сертификатлаш  
органи

**en** - certification  
authority, CA

1. Орган, которому одним или более пользователями доверено создавать, и распределять сертификаты открытых ключей.

2. Объект, которому доверено (в контексте политики обеспечения безопасности) создавать сертификаты безопасности, содержащие один или более классов данных, относящихся к обеспечению безопасности.



## О

1. Битта ёки бир нечта фойдаланувчи томонидан очик калитлар сертификатларини тузиш ва тақсимлаш ишониб топширилган орган.

2. Хавфсизликни таъминлашга тааллуқли бўлган маълумотларнинг бир ёки ундан ортиқ классини ичига олган хавфсизлик сертификатларини тузиш ишониб топширилган объект (хавфсизликни таъминлаш сиёсати контекстида).

### **Ответ ожидаемый**

**uz** - кутилган жавоб

**en** - expected

response, XRES

Отклик, вычисляемый в сети с использованием того же алгоритма, что и ответ мобильной станции. Если XRES и SRES совпадают, то аутентификация завершается успешно.

Мобил станциянинг жавоби каби алгоритмдан фойдаланиб, тармоқда ҳисоблаб чиқариладиган жавоб. Агар XRES ва SRES мос келса, аутентификация қилиш муваффақиятли тугайди.

### **Отказ в обслуживании**

**uz** - хизмат кўра-

тишни рад этиш

**en** - denial of service,

DoS

1. Прекращение санкционированного доступа к ресурсам или задержка выполнения операций, критичных ко времени.

2. Любое действие или последовательность действий, которая приводит любую часть системы к выходу из строя, при котором та перестаёт выполнять свои функции. Причиной может быть несанкционированный доступ, задержка в обслуживании и т.д.

3. Отказ в предоставлении ресурсов законным пользователям вследствие нарушения режима сетевого обслуживания. Обычно возникает при введении в сеть фиктивного трафика или ложных запросов, которые, хотя и отбрасываются, но загружают сеть ненужной информацией.

1. Ресурслардан рухсат этилган тарзда фой-

## О

далана олишнинг тўхтатилиши ёки вақтга нисбатан критик операциялар бажарилишининг кечикиши.

2. Тизимнинг ҳар қандай қисмини сафдан чиқарадиган ва бунда тизим ўз функцияларини бажаришни тўхтатадиган ҳар қандай ҳаракат ёки ҳаракатлар кетма-кетлиги. Бунинг сабаби рухсат этилмаган тарзда фойдалана олиш, хизмат кўрсатишдаги кечикишлар ва б.к. бўлиши мумкин.

3. Тармоқ хизмат кўрсатиш режимининг бузилиши натижасида ресурсларнинг қонуний фойдаланувчиларга тақдим этилишини рад этиш. Одатда, тармоққа сохта трафик ёки ёлғон сўровлар киритилганда пайдо бўлади, гарчи улар олиб ташлансада, тармоқни кераксиз ахборот билан банд қилиб кўяди.

### **Отказ в обслуживании распределенный**

**uz** - хизмат кўрсатишни тақсимланган рад этиш  
**en** - Distributed Denial of Service, DDoS

Нарушение работы сети, обусловленное одновременной атакой злоумышленников на разные ее элементы.

Тармоқ ишининг жинойткорларнинг, тармоқнинг турли элементларига бир вақтда ҳужум қилиши билан боғлиқ бўлган бузилиши.

### **Отказ от авторства**

**uz** - муаллифликни рад этиш  
**en** - refusal of authorship

Отрицание причастности к какому-либо документу или сообщению.

Қандайдир ҳужжат ёки хабарга алоқадорликни рад этиш.

### **Отклик ожидаемый**

**uz** - кутилган жавоб  
**en** - Signed Response, SRES

Ответ мобильной станции на полученное случайное число RAND.

Олинган RAND тасодифий сонига мобил станциянинг жавоби.

## О

**Отладчик**  
uz - созловчи  
en - debugger

Программа или устройство, предназначенное для выявления ошибок в программном обеспечении.

Дастурий таъминотдаги хатоларни аниқлаш учун мўлжалланган дастур ёки курилма.

**Отношение**  
uz - муносабат  
en - relationship

Воспринимаемая связь между объектами в предметной области.

Предмет соҳасидаги объектлар ўртасида қабул қилинадиган алоқадорлик (боғланиш).

**Отношения доверительные**  
uz - ишончли муносабатлар  
en - trust relationships

Несимметричная логическая связь между двумя доменами, позволяющая системе безопасности одного домена (доверяющего, trusting) использовать в качестве субъектов учетные записи другого домена (доверяемого, trusted).

Икки домен ўртасидаги, бир домен (ишонувчи, trusting) хавфсизлик тизимида бошқа домен (ишонч билдирилаётган, trusted) ҳисоб ёзувларидан субъект сифатида фойдаланиш имконини берадиган носимметрик мантиқий алоқа.

**«Отпечаток» цифровой**  
uz - рақамли «из»  
en - digital fingerprint

Характеристика элемента данных, например, криптографическое контрольное значение или результат выполнения односторонней функции хэширования в отношении данных.

Маълумотлар элементининг характеристикаси, масалан, криптографик назорат қиймати ёки маълумотларга нисбатан бир томонлама хэшлаш функциясини бажариш натижаси.

**Оценка безопас-**

Проверка системы с целью определения

**ности**

**uz** - хавфсизликни баҳолаш

**en** - security evaluation

степени ее соответствия установленной модели защиты, стандарту обеспечения защиты и техническим условиям.

Тизимни, белгиланган муҳофаза моделига, муҳофаза қилишни таъминлаш стандарти ва техник шартларга мос келиш даражасини аниқлаш мақсадида, текшириш.

**Оценка качества программного изделия**

**uz** - дастурий маҳсулот сифатини баҳолаш

**en** - program quality estimation

Комплекс мероприятий, включающий выбор показателей качества, отбор или разработку методов определения количественных значений этих показателей, установление базовых значений показателей, расчет реальных значений показателей, сравнение базовых значений с расчетными.

Сифат кўрсаткичлари танланишини, бу кўрсаткичларнинг миқдор қийматларини танлаш ва аниқлаш методлари ишлаб чиқилишини, кўрсаткичларнинг базавий қийматлари белгиланишини, кўрсаткичларнинг ҳақиқий қийматларини ҳисоблаш, базавий қийматларни ҳисобланган қийматлар билан таққослашни ичига оладиган тадбирлар комплекси.

**Оценка риска**

**uz** - риск (эхтимолий хавф)ни баҳолаш

**en** - risk assessment

1. Количественная или качественная оценка повреждения, которое может произойти, если вычислительная система не защищена от определенных угроз.

2. Метод анализа угроз и слабых сторон, известных и предполагаемых, позволяющий определить размер ожидаемого ущерба и степень его приемлемости для работы системы (сети).

3. Идентификация рисков, выбор параметров для их описания и получения оценок по этим параметрам.

## О

1. Ҳисоблаш тизими маълум бир таҳдидлардан муҳофазаланмаганда юз бериши мумкин бўлган шикастланишни микдор ёки сифат жиҳатдан баҳолаш.

2. Маълум бўлган ва тахмин қилинаётган таҳдидлар ва заиф томонларни таҳлил қилиш методи. Кутилаётган зарар микдорини ва унинг тизим иши учун мақбуллик даражасини аниқлаш имконини беради.

3. Риск (эҳтимолий хавф)ларни идентификация қилиш, уларни тавсифлаш учун параметрлар танлаш ва бу параметрлар бўйича баҳо олиш.

### Очистка

uz - тозалаш

en - clearing

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.

Категориялаштирилган маълумотларни муайян махфийлик грифига ҳамда муҳофаза қилиш категориясига эга бўлган маълумот ташувчига, уни худди шундай махфийлик грифи ва муҳофаза қилиш категориясидаги маълумотларни бир неча марта ёзиб олишда фойдаланиш мумкин бўлиши учун, қайта ёзиш.

### Ошибка (преднамеренная) умышленная

uz - атайлаб (қасдан) қилинган хато

en - intentional error

Ошибка, преднамеренно внесенная в программу или данные.

Дастур ёки маълумотларга қасдан қилинган хато.

### Ошибка данных

uz - маълумотлар-

Ошибочное представление одного или нескольких исходных данных, которое может

## О

нинг хатолиги  
en - data error

стать причиной аварийного завершения программы либо оказаться необнаруженным, но результаты нормально завершившейся программы будут при этом неверными.

Битта ёки бир нечта бошланғич маълумотнинг хато такдим этилиши. Дастур авариявий тугалланишига сабабчи бўлиши ёки аниқланмай қолиши мумкин, ammo нормал тугалланган дастур натижалари бу ҳолда нотўғри бўлади.

**Ошибка кратко-  
временная**  
uz - қисқа муддатли  
хато  
en - soft error

Ошибка из-за случайных обстоятельств, сбой.

Тасодифий ҳолатлар натижасида юзага келадиган хато, узилиш.

**Ошибка  
невосстанавли-  
ваемая**  
uz - тиклаб бўлмайдиган хато  
en - unrecoverable  
error

Ошибка, последствия которой не могут быть устранены средствами вычислительной системы автоматически, и требуют вмешательства оператора.

Оқибатларини ҳисоблаш тизими воситалари билан автоматик равишда бартараф этиб бўлмайдиган, операторнинг аралашуви талаб этиладиган хато.

**Ошибка некор-  
ректируемая**  
uz - тузатиб  
бўлмайдиган хато  
en - uncorrectable  
error

Ошибка в сообщении, которая не может быть исправлена средствами корректирующего кода.

Хабардаги тузатувчи код воситалари билан тузатиш мумкин бўлмаган хато.

**Ошибка неповто-  
ряющаяся (нерегу-  
лярная, переме-  
жающаяся, слу-  
чайная)**

Несистематическая ошибка, возникающая вследствие самоустраняющихся машинных отказов, сбоев и других случайных обстоятельств.

## О

**uz** - такрорланмай-  
диган (мунтазам  
бўлмаган, вақт-вақти  
билан учрайдиган,  
тасодифий) хато  
**en** - temporary (in-  
termittent, soft, tran-  
siet) error

**Ошибка семанти-  
ческая**  
**uz** - семантик хато  
**en** - semantic error

**Ошибка фаталь-  
ная**  
**uz** - фатал хато  
**en** - fatal error

**Ошибка четности**  
**uz** - жуфтлик хато-  
си  
**en** - parity error

**Пакеты-убийцы**  
**uz** - котил пакетлар  
**en** - package killers

Ўз-ўзидан бартараф бўладиган машина бу-  
зилишлари, тўхтаб қолишлар ва бошқа тасо-  
дифий ҳолатлар оқибатида пайдо бўлувчи  
номунтазам хато.

Ошибка программирования, возникающая из-  
за непонимания смысла, значения или действия  
той или иной конструкции программирования.

Дастурлашдаги хато дастурлаш у ёки бу  
конструкциясининг маъносини, аҳамиятини  
ёки ишини тушунмаслик туфайли юзага  
келади.

Ошибка, при появлении которой дальней-  
шее выполнение программы приводит к бес-  
смысленным результатам.

Пайдо бўлиши дастурнинг бажарилишида  
ноаник (маъносиз) натижаларга олиб кела-  
диган хато.

Ошибка в данных, обнаруживаемая в про-  
цессе их хранения или передачи путем  
контроля на четность.

Маълумотлардаги, уларни сақлаш ёки  
жуфтликни назорат қилиш орқали узатиш  
жараёнида аниқланадиган хато.

## П

Метод вывода из строя информационной  
системы путем посылки ей Ethernet- или IP-  
пакетов, которые используют ошибки в  
сетевых программах для аварийного завер-  
шения работы этой системы.

## П

Тизимнинг ишини авариявий тугатиш учун тармоқ дастурларидаги хатолардан фойдаланадиган Ethernet ёки IP-пакетларини юбориш йўли билан ахборот тизимини ишдан чикариш методи.

### **Память с защитой**

**uz** - химояга эга хотира

**en** - protected storage

Память, имеющая специальные средства защиты от несанкционированного доступа к любой из ее ячеек.

### **Память только для записи**

**uz** - фақат ёзиш учун хотира

**en** - memory for write only

Исталган ячейкасига рухсат этилмаган тарзда кира олишдан муҳофаза қилувчи махсус воситалари бўлган хотира.

Тип памяти со следующими свойствами: после записи новой информации прежняя может быть восстановлена только с помощью внутренних механизмов самого чипа; данные никогда не распространяются за пределы чипа и не могут появиться на шинах, внешних по отношению к чипу.

Янги ахборот ёзилгандан сўнг олдингиси фақат чипнинг ички механизмлари ёрдамида тикланиши мумкин бўлган; маълумотлар ҳеч қачон чипдан ташқарида тарқатилмайдиган ва чипга нисбатан ташқи ҳисобланадиган шиналарда пайдо бўлмай-диган хотира тури.

### **Паролирование**

**uz** - пароллаштириш

**en** - determination of password

Один из методов ограничения доступа к компьютерной системе и ее файлам.

### **Пароль**

**uz** - паролъ

**en** - password

Компьютер тизими ва унинг файлларига кира олишни чеклаш методларидан бири.

1. Последовательность символов, которая используется как информация аутентификации.
2. Идентификатор субъекта доступа, являющийся его (субъекта) секретом.



## П

3. Секретная информация аутентификации, обычно представляющая собой строку знаков, которой должен обладать пользователь для доступа к защищенным данным.

4. Средство идентификации доступа, представляющее собой кодовое слово в буквенной, цифровой или буквенно-цифровой форме, которое вводится в ЭВМ перед началом диалога с нею с клавиатуры терминала или при помощи идентификационной (кодовой) карты.

1. Аутентификация қилиш ахбороти сифатида фойдаланиладиган белгилар кетмакетлиги.

2. Эркин фойдаланиш субъектининг идентификатори бўлиб, субъектнинг сири ҳисобланади.

3. Фойдаланувчининг муҳофаза қилинган маълумотлардан эркин фойдаланиши учун эга бўлиши керак бўлган белгилар сатрини ўзида акс эттирувчи махфий аутентификация қилиш ахбороти.

4. Электрон ҳисоблаш машинасига терминал клавиатурасидан ёки идентификацион (кодли) карта ёрдамида киритиладиган, ҳарф, ҳарф-рақам ёки рақам шаклидаги кодли сўзни ўзида ифодаловчи, эркин фойдаланишни идентификацияловчи восита.

**Пароль главный**  
**uz** - асосий пароль  
**en** - main password

1. Корневое слово, являющееся общим для определенного набора паролей.

2. Пароль, предназначенный для защиты каталога паролей.

1. Паролларнинг маълум бир тўплами учун умумий бўлган ўзак сўз.

2. Пароллар каталогини муҳофаза қилиш учун мўлжалланган пароль.

## П

### **Пароль одноразовый**

**uz** - бир мартали  
пароль  
**en** - single-use  
password

Пароль с очень коротким сроком действия, обычно изменяемый после каждого входа в сеть.

Тармоққа ҳар бир киришдан сўнг ўзга-радиған, амал қилиш муддати жуда қисқа бўлган пароль.

### **Перебор номеров циклический**

**uz** - рақамларни  
циклик саралаш  
**en** - tumbling

Скрытное клонирование с циклическим перебором номеров телефонов-двойников, при котором каждый последующий вызов осуществляется с новым номером.

Ўхшаш телефонларнинг рақамларини циклик саралаш билан ёпиқ клонлаш, унда ҳар бир кейинги чақирув янги рақам билан амалга оширилади.

### **Перебор полный**

**uz** - тўлиқ саралаш  
**en** - exhaustive  
search

Основной метод поиска правильного криптографического ключа из множества всех возможных ключей путем его полного перебора. Число возможных ключей можно сократить, если найдены уязвимости алгоритма шифрования или выработки ключей.

Тўғри криптографик қалитни барча мумкин бўлган қалитлар ичидан уни тўлиқ саралаш йўли билан излашнинг асосий методи. Шифрлаш алгоритми ёки қалитларни ишлаб чиқишда заифликлар топилганда қалитлар сонини қисқартириш мумкин бўлади.

### **Передача права**

**uz** - ҳуқуқни бериш  
**en** - assignment of  
right

Законная передача владельцем права интеллектуальной собственности другому лицу.

Интеллектуал мулкчилик ҳуқуқининг эгаси томонидан бошқа шахсга қонуний берилиши.

### **Перемешивание**

**uz** - аралаштириб  
юбориш  
**en** - confusion

Свойство шифрующего преобразования усложнять взаимосвязи между элементами данных, что затрудняет восстановление функциональных и статистических связей

## II

между открытым текстом, ключом и шифротекстом.

Шифрловчи ўзгартиришнинг маълумотлар элементлари ўртасидаги алоқадорликни мураккаблаштириш хоссаси. Бу нарса очик матн, калит ва шифрматн ўртасидаги функционал ва статистик боғланишнинг тикланишини қийинлаштиради.

### Переполнение

**uz** - тўлиб кетиш  
**en** - overflow

Случайный или умышленный ввод большого объема данных, результатом которого является отказ в обслуживании.

Маълумотларнинг катта ҳажмини тасодифан ёки қасддан киритиш, унинг натижасида хизмат кўрсатишнинг рад этилиши юз беради.

### Переполнение-SYN

**uz** - SYN тўлиб кетиш  
**en** - SYN overflow

Метод вывода системы из строя путем посылки ей такого числа SYN-пакетов, которое не может обработать сетевой драйвер.

Тармоқ драйвери қайта ишлай олмайдиган микдорда SYN пакетларни юбориш орқали тизимни ишдан чиқариш методи.

### Перестановка

**uz** - ўрнини (тартибини) алмаштириш  
**en** - permutation

1. Криптографическая операция, связанная с изменением порядка следования отдельных битов или символов в блоке данных.

2. Шифрование, при котором биты или символы переставляются по некоторой схеме.

*Примечание: Полученный шифротекст называется шифром перестановки.*

1. Маълумотлар блокадаги айрим битлар ёки символларнинг ўтиш тартибини ўзгартириш билан боғлиқ криптографик операция.

2. Битлар ёки белгилар маълум схема бўйича алмаштириладиган шифрлаш.

## П

*Изоҳ: Олинган шифрланган матн ўрнини ал-  
маштириш шифри деб аталади.*

### **Перехват информации**

**uz** - ахборотни  
қўлга киритиш  
**en** - wiretapping

Тайное подключение нелегального устройства к какой-либо части линии телекоммуникаций, чтобы получать, модифицировать или вставлять данные.

Маълумотларни олиш, ўзгартириш ёки киритиш мақсадида телекоммуникациялар линиясининг бирор-бир қисмига яширин қурилмани билдирмасдан улаш.

### **Перехват информации активный**

**uz** - ахборотни актив  
тутиб қолиш  
**en** - active  
wiretapping

Подключение нелегального устройства к линии телекоммуникаций с целью модифицировать или вставить данные.

Маълумотларни ўзгартириш ёки киритиш мақсадида телекоммуникациялар линиясига яширин қурилмани улаш.

### **Перехват информации пассивный**

**uz** - ахборотни пассив  
тутиб қолиш  
**en** - passive  
wiretapping

Подключение нелегального устройства к линии телекоммуникаций для получения данных.

Маълумотлар олиш мақсадида телекоммуникациялар линиясига яширин қурилмани улаш.

### **Перехват сообщений**

**uz** - хабарларни  
тутиб қолиш  
**en** - message  
wiretapping

Несанкционированное подключение специального терминала к линии телекоммуникаций, прием и использование сообщений, циркулирующих между абонентскими пунктами и ЭВМ.

Махсус терминални телекоммуникациялар линиясига рухсатсиз улаш, абонент пунктлари билан электрон ҳисоблаш машинаси ўртасида айланадиган хабарларни қабул қилиш ва улардан фойдаланиш.

## П

**Перечень сведений, подлежащих засекречиванию**

**uz** - махфийлашти-рилиши зарур

бўлган маълумотлар рўйхати

**en** - list of information to be classified as secret

**Период действия ключа**

**uz** - калитнинг амал қилиш даври

**en** - life cycle

**Период доступа**

**uz** - эркин фойдаланиш даври

**en** - access period

**Печать**

**uz** - мухр

**en** - seal

Документ, утвержденный в установленном порядке, определяющий степень секретности сведений, разглашение которых может нанести ущерб интересам Республики Узбекистан.

Белгиланган тартибда тасдиқланган, тарқатилиши Ўзбекистон Республикаси манфатларига зиён етказиши мумкин бўлган маълумотларнинг махфийлик даражасини белгилловчи ҳужжат.

Интервал времени, в течение которого гарантируются необходимая защищенность без смены криптографического ключа.

Вақт интервали, унинг мобайнида криптографик калит алмаштирилмасдан зарур муҳофазаланганлик кафолатланади.

Временной интервал, в течение которого действуют указанные права на доступ.

Эркин фойдаланиш учун кўрсатилган ҳуқуқлар амал қиладиган вақт интервали.

Криптографическое контрольное значение, которое обеспечивает поддержку целостности, но не защищает от подлога, осуществляемого получателем (т.е. не обеспечивает фиксацию авторства).

Криптографик назорат қиймати бўлиб, яхлитлик сакланиб туришини таъминлайди, лекин олувчи томонидан амалга ошириландиган қалбакилашти-ришдан муҳофаза қила олмайди (яъни, муаллиф-лик қайд этилишини таъминлай олмайди).

**Пиггибекинг физический**

Несанкционированный проход через контролируемую дверь вслед за полномочным

## П

- uz** - жисмоний пиг-гибекинг  
**en** - to tailgate  
лицом.  
Ваколатли шахс ортидан назорат қилинадиган эшик орқали рухсат этилмаган тарзда ўтиш.
- Пиггибекинг электронный**  
**uz** - электрон пиггибекинг  
**en** - electronic piggyback  
Несанкционированный доступ к системе обработки данных по легальному соединению полномочного пользователя.  
Ваколатли фойдаланувчининг қонуний боғланиши орқали маълумотларни қайта ишлаш тизимидан рухсат этилмаган тарзда фойдалана олиш.
- Пират телефонный (взломщик телефонных сетей)**  
**uz** - телефон қарқочиси (телефон тармоқларини бузувчи)  
**en** - phreaker  
Мошенник, являющийся, как правило, профессиональным связистом с навыками хакера. Создает электронные устройства, позволяющие ему подключаться к телефонным сетям и использовать их ресурсы без надлежащей оплаты.  
Хакер малакасига эга профессионал алоқачи бўлган фирибгар. Телефон тармоқларига уланиш ва уларнинг ресурсларидан тегишли тўловларсиз фойдаланиш имконини берадиган электрон қурилмаларни ярати.
- Пиратство программное**  
**uz** - дастурий қарқочилик  
**en** - software piracy  
Неправомерное использование, копирование или распространение лицензионных программных продуктов, являющихся авторским произведением.  
Муаллифлик асари ҳисобландиган лицензион дастурий маҳсулотлардан ноқонуний фойдаланиш, нусха кўчириш ёки тарқатиш.
- План обеспечения непрерывной работы и восстановления**  
План реагирования на опасные ситуации, резервного копирования и последующих восстановительных процедур, являющийся

## П

### ления функционирования

**uz** - узлуксиз ишлашни таъминлаш ва тиклаш режаси  
**en** - contingency plan (backup plan, recovery plan)

частью программы защиты и обеспечивающий доступность основных ресурсов системы и непрерывность обработки в кризисных ситуациях.

Муҳофаза қилиш дастурининг бир қисми ҳисобланадиган ҳамда тизимнинг асосий ресурсларидан фойдаланишни ва кризисли вазиятларда қайта ишлашнинг узлуксизлигини таъминловчи, хавфли вазиятларга жавоб бериш, резерв нусха кўчириш ва кейинги тиклаш процедуралари режаси.

### Плата копирования

**uz** - нусха кўчириш платаси  
**en** - copy card

Электронное устройство, которое после установки в ЭВМ позволяет копировать защищенное программное обеспечение из оперативной памяти на диск.

Электрон ҳисоблаш машинасига ўрнатилгандан сўнг оператив хотирадан дискка муҳофазаланган дастурий таъминотни кўчириш имконини берадиган электрон қурилма.

### Повтор

**uz** - такрор(лаш)  
**en** - replay

Простейший вид сетевой атаки, когда злоумышленник перехватывает сообщение и повторяет его, не изменяя, в более позднее время.

Тармоққа қилинадиган ҳужумнинг оддий тури, бунда жинойткор хабарни тутиб олади ва уни ўзгартирмасдан, бирмунча кечроқ такрорлайди.

### Подглядывание из-за плеча

**uz** - елка оша яширинча қараш  
**en** - keeking behind shoulder

Кража паролей или PIN-кодов путем наблюдения за их набором на клавиатуре.

Пароллар ёки PIN-кодларни уларнинг клавиатурада терилишини кузатиш йўли билан ўғирлаш.

### Подделка

Модификация злоумышленником содержа-

## П

**uz** - сохталашти-  
риш  
**en** - tampering

### Подделка информации

**uz** - ахборотни  
сохталаштириш  
**en** - data corruption

### Подотчетность

**uz** - ҳисоб бериш-  
лик  
**en** - accountability

ния перехваченных пакетов, приводящая к потере целостности.

Жинояткор томонидан тутиб олинган пакетлар мазмунининг, уларнинг яхлитлиги бузилишига олиб келадиган тарзда, ўзгартирилиши.

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

Ахборотни, рақобатчи олдиди маълум фойда (афзаллик) олиш ёки унга зарар етказиш мақсадида, техник воситалар билан қайта ишлашда, атайин рұхсат этилмаган тарзда ўзгартириш.

1. Свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта.
2. Свойство автоматизированной системы, позволяющее фиксировать деятельность ее субъектов и ассоциировать их с индивидуальными идентификаторами для последующего выявления нарушений безопасности и ответственных за эти нарушения.
3. Возможность для ответственных за защиту информации лиц восстанавливать ход нарушения или попытки нарушения безопасности информационной системы.
4. Свойство реальной открытой системы, заключающееся в способности контролировать действия пользователей и ресурсов с целью последующего выявления нарушений безопасности и ответственных за эти нарушения.



## П

1. Ҳар қандай мантикий объектнинг ҳаракатларини қатъий кузатишни таъминлайдиган хусусият.

2. Автоматлаштирилган тизимнинг тизим субъектлари фаолиятини қайд қилишга ҳамда уларни хавфсизлик бузилишлари ва бу бузилишлар учун жавобгарларни келгусида аниқлаш учун уларнинг индивидуал идентификаторлари билан ассоциациялаш имконини берувчи хусусияти.

3. Ахборотнинг муҳофаза қилиниши юзасидан жавобгар бўлган шахслар учун ахборот тизими хавфсизлиги бузилиш жараёнини ёки бузишга уринишларни тиклаш имконияти.

4. Реал очик тизимнинг, хавфсизлик бузилишларини ва улар юзасидан жавобгарларни аниқлаш мақсадида, фойдаланувчиларнинг ҳаракатини ва ресурсларни назорат қилишида ифодаланадиган хусусияти.

### Подпись бесспорная

uz - аниқ имзо  
en - indisputable signature

Схема цифровой подписи, использующая протокол отрицания, который позволяет предотвратить отказ подписывающего от своего сообщения.

Инкор қилиш протоколидан фойдаланиладиган рақамли имзо схемаси имзо чекувчининг ўз хабарини инкор этишининг олдини олиш имконини беради.

### Подпись групповая

uz - гуруҳий имзо  
en - group signature

Схема цифровой подписи, предложенная в 1991 г. Чомом и Ван Хейстом, позволяющая любому члену группы подписать сообщение таким образом, чтобы при проверке можно было установить, что сообщение подписано одним из членов группы, без конкретизации личности подписывающего.

1991 йилда Чом ва Ван Хейст томонидан

## II

таклиф қилинган рақамли имзо схемаси, гуруҳнинг исталган аъзосига хабарни, текшириш пайтида, хабар гуруҳ аъзоларидан бири томонидан имзо чекувчининг шахсини аниқлаштирилмасдан имзоланганини аниқлаш мумкин бўладиган тарзда имзолаш имконини беради.

**Подпись кода**  
**uz** - код ёзуви  
**en** - code signature

Механизм, позволяющий подписывать программное обеспечение, распространяемое по сетям общего пользования. Это позволяет аутентифицировать автора программного обеспечения и гарантировать, что в процессе передачи код не модифицировался.

Умумий фойдаланиш тармоқлари бўйлаб тарқатиладиган дастурий таъминотни имзолаш имконини берувчи механизм. Бу дастурий таъминот муаллифини аутентификация қилиш ва узатиш жараёнида коднинг ўзгартирилмаслигини кафолатлаш имконини беради.

**Подпись самопроверяющаяся**  
**uz** - ўз-ўзини текшириш имзоси  
**en** - self-verifying signature

Цифровая подпись, подлинность которой может быть проверена в любое время без согласия подписывающего лица. К этой категории может быть отнесена любая цифровая подпись с открытым ключом.

Ҳақиқийлиги имзо чекувчи шахсининг розилигисиз исталган вақтда текширилиши мумкин бўлган рақамли имзо. Бу категорияга очиқ қалитли исталган рақамли имзо киритилиши мумкин.

**Подпись слепая**  
**uz** - кўр-кўрона имзо  
**en** - blind signature

Механизм электронной цифровой подписи, используемый в платежной системе DigiCash и основанный на применении случайного множителя (blinding factor). DigiCash тўлов тизимида ишлатиладиган ва

## II

тасодифий кўпайтирувчини (blinding factor) қўллашга асосланган электрон рақамли имзо механизми.

### Подпись цифровая

uz - рақамли имзо

en - digital signature

1. Данные, добавляемые к сообщению и позволяющие получателю сообщения проверить подлинность отправителя.

2. Последовательность данных, добавляемая к блоку данных или к результату его криптографического преобразования, которая позволяет получателю данных проверить источник и целостность блока данных, а также защиту от подлога или подделки.

1. Хабарга кўшимча қилинадиган ҳамда хабар олувчига жўнатувчининг ҳақиқийлигини текшириш имконини берувчи маълумотлар.

2. Маълумотлар блокига ёки уни криптографик қайта ўзгартириш натижасига кўшимча қилинадиган маълумотлар кетмакетлиги, у маълумотлар олувчисига манба ва маълумотлар блокининг яхлитлигини текшириш, шунингдек, сохталаштиришдан ёки алмаштиришдан муҳофаза қилиш имконини беради.

### Подпись цифровая

#### одноразовая

uz - бир мартали

рақамли имзо

en - one-shot digital signature

Схема, в которой для любого сообщения цифровая подпись может быть использована только один раз, т.е. для каждого нового сообщения требуется новая пара ключей. Достоинством такой схемы является быстрота, недостатком – необходимость опубликования большого количества информации (открытых ключей), так как каждая подпись используется только один раз.

Ҳар қандай хабар учун рақамли имзо фақат бир марта ишлатилиши мумкин бўлган схема, яъни ҳар бир янги хабар учун калит-

## П

ларнинг янги жуфти талаб қилинади. Бундай схеманинг афзаллиги унинг тезкорлиги ҳисобланади, камчилиги — катта миқдордаги ахборотни (очиқ калитларни) эълон қилиш зарурлиги, чунки ҳар бир имзо фақат бир марта ишлатилади.

**Подпись цифровая электронная, ЭЦП**

**uz** - электрон рақамли имзо, ЭРИ  
**en** - digital signature

Механизм, позволяющий на основе криптографических методов надежно установить авторство и подлинность информации (сообщения или документа).

Криптографик методлар асосида муаллифликни ва ахборот (хабар ёки ҳужжат)нинг ҳақиқийлигини ишончли белгилашга имкон берувчи механизм.

**Подслушивание**  
**uz** - яширин эшитиш

**en** - eavesdropping

1. Перехват злоумышленником передаваемой по сети информации с целью выявления и последующей эксплуатации слабых мест системы защиты.

2. Любые действия, связанные с перехватом конфиденциальной информации, в том числе за счет приема излучений по побочным каналам.

1. Жинояткор томонидан тармоқ бўйлаб узатиладиган ахборотни, муҳофаза тизимининг заиф жойларини аниқлаш ва кейинчалик ундан фойдаланиш мақсадида, қўлга киритиш.

2. Конфиденциал ахборотни қўлга киритиш билан боғлиқ, ҳар қандай ҳаракатлар шу жумладан, қўшни каналлар орқали нурлашишларни қабул қилиш ҳисобига.

**Подстановка**  
**uz** - ўрнига қўйиш  
**en** - substitution

1. Шифрование, при котором последовательность битов или символов заменяется другой последовательностью битов или символов.

*Примечание: Полученный шифротекст называется*

## II

*ется шифром подстановки.*

2. Криптографическая операция, связанная с замещением одного блока другим и использующая определенный код.

1. Битлар ёки символлар кетма-кетлиги бошқа битлар ёки символлар кетма-кетлиги билан алмаштириладиган шифрлаш.

*Изоҳ: Олинган шифрланган матн ўрнига қўйиш шифри деб аталади.*

2. Бир блокни бошқаси билан алмаштириш билан боғлиқ ва маълум коддан фойдаланувчи криптографик операция.

### Подстановка трафика

**uz** - трафикни

ўрнига қўйиш

**en** - traffic padding

1. Установление поддельных соединений, генерация фальшивых блоков данных и/или отдельных фальшивых данных внутри блоков данных.

2. Генерирование ложных событий связи, ложных блоков данных и/или ложных данных в пределах блоков данных.

1. Сохта уланишларни аниқлаш, қалбаки маълумотлар блокларини ва/ёки маълумотлар блоки ичидаги алоҳида қалбаки маълумотларни генерациялаш.

2. Маълумотлар блоки доирасида нотўғри алоқа воқеаларини, нотўғри маълумотлар блокларини ва/ёки нотўғри маълумотларни генерациялаш.

### Подсчет побитовый

**uz** - битма-бит

ҳисоблаш

**en** - bit counting

Метод защиты от копирования, при котором диск распознается как оригинал, если некоторая дорожка (или другая область) содержит определенное число битов.

Нусха олинисдан муҳофаза қилиш методи бўлиб, қандайдир йўлка (ёки бошқа соҳа) битларнинг муайян сонини ичига олганда, диск оригинал сифатида аниқланади.

## П

**Подтверждение подлинности**  
**uz** - ҳақиқийликни тасдиқлаш  
**en** - authentication

Механизм, направленный на подтверждение подлинности и предусматривающий обмен информацией.

Ҳақиқийликни тасдиқлашга йўналтирилган ва ахборот алмашинуви кўзда тутилган механизм.

**Показатель защищенности средств вычислительной техники**  
**uz** - ҳисоблаш техникаси воситаларининг муҳофазаланганлик кўрсаткичи  
**en** - hardware protection indicator

Характеристика средств вычислительной техники, отражающая показатели защищенности и описываемая определенной группой требований, варьируемых по уровню и глубине в зависимости от класса защищенности средств вычислительной техники.

Ҳисоблаш техникаси воситаларининг, уларнинг муҳофазаланганлик классига боғлиқ ҳолда, даража ва кенглик бўйича ўзгартирилган талабларнинг маълум гуруҳи билан тавсифланган ва муҳофазаланганлик кўрсаткичларини ақс эттирувчи характеристикаси.

**Показатель эффективности защиты информации**  
**uz** - ахборотни муҳофаза қилишнинг самарадорлик кўрсаткичи  
**en** - efficiency factor of information security

Мера или характеристика для оценки эффективности защиты информации.

Ахборотни муҳофаза қилиш самарадорлигини баҳолаш ўлчови ёки характеристикаси.

**Поле (диска) адресное**  
**uz** - адресли (диск) майдони  
**en** - address field (disk)

Начальная область сектора на диске, в которой указано число дорожек и секторов.

Дискдаги секторнинг йўлкалар ва секторлар сони кўрсатилган бошланғич соҳаси.

**Поле данных**

Часть дискового пространства (сектора) для

## II

**uz** - маълумотлар  
майдони  
**en** - data field

размещения данных, которому предшествует адрес.

**Поле управления  
аутентификацией**  
**uz** - аутентифика-  
цияни бошқариш  
майдони  
**en** - authentication  
management field,  
AMF

Поле данных, используемое для проверки аутентичности сообщения.

**Политика безо-  
пасности**  
**uz** - хавфсизлик  
сиёсати  
**en** - security policy

Хабарнинг аутентиклигини (хакикийлигини) текшириш учун қўлланиладиган маълумотлар майдони.

1. План или программа действий, принятая для обеспечения компьютерной безопасности.
2. Набор законов, правил и практических рекомендаций, на основе которых строятся управление, защита и распределение защищаемой информации в системе. Она охватывает все особенности процесса обработки информации, определяя поведение системы в различных ситуациях.
3. Набор правил, определяющих процедуры и механизмы обеспечения безопасности заданного подмножества объектов и субъектов безопасности.
4. Формальное определение критериев, особенно оперативных, которыми следует руководствоваться при обеспечении защиты системы от известных угроз.
5. Свод законов, норм, правил, практических рекомендаций и приёмов, которые регулируют в данной организации обработку, защиту и распространение значимой информации.

## II

1. Компьютер хавфсизлигини таъминлаш учун қабул қилинган ҳаракатлар режаси ёки дастури.

2. Қонунлар, қоидалар ва амалий тавсияномалар тўплами, унга асосан тизимдаги муҳофаза қилинаётган ахборотни бошқариш, муҳофаза қилиш ва тақсимлаш йўлга қўйилади. У турли вазиятларда тизим ўзини қандай тутишини белгилаган ҳолда, ахборотни қайта ишлаш жараёнининг барча хусусиятларини қамраб олади.

3. Хавфсизлик объектлари ва субъектлари берилган кўплигининг хавфсизлигини таъминлаш процедура ва механизмларини белгиловчи қоидалар тўплами.

4. Тизимнинг маълум таҳдидлардан муҳофаза қилинишини таъминлашда таяниш мумкин бўлган критерийларнинг, айниқса, оператив критерийларнинг формал белгиланиши.

5. Ташкилотда аҳамиятли ахборотнинг қайта ишланишини, муҳофаза қилинишини ва тарқатилишини тартибга соладиган қонунлар, нормалар, қоидалар, амалий тавсиялар ва усуллар тўплами.

**Политика безопасности идентификационная**  
**uz** - идентификацион хавфсизлик сиёсати  
**en** - identity-based security policy

Политика безопасности, основанная на идентифицирующих свойствах и/или атрибутах пользователей сети, группы пользователей сети, используемых ресурсов сети.

Фойдаланиладиган тармоқ ресурсларининг, тармоқ фойдаланувчиларининг, фойдаланувчилар гуруҳининг идентификацияловчи хоссалари ва/ёки атрибутларига асосланган хавфсизлик сиёсати.

**Политика безопасности инструкционная**  
**uz** - инструкция

Методика безопасности, основанная на общих правилах, обязательных для всех пользователей автоматизированной информационной системы (АИС).



## II

хавфсизлик сиёсати  
en - rule-based security policy

**Политика информационной безопасности сети телекоммуникаций общего пользования**

uz - умумий фойдаланишдаги телекоммуникациялар тармоғининг ахборот хавфсизлиги сиёсати

en - public switched telecommunications network information security policy

**Полномочие**  
uz - ваколат  
en - authority

Автоматлаштирилган ахборот тизими (ААТ) барча фойдаланувчилари учун мажбурий бўлган умумий қоидаларга асосланган хавфсизлик методикаси.

Совокупность требований и правил для объекта (объектов) информационной безопасности сети телекоммуникаций общего пользования, выработанных администрацией сети, в целях противодействия определенным угрозам информационной безопасности сети, с учетом ценности защищаемых ресурсов и стоимости системы обеспечения информационной безопасности сети телекоммуникаций общего пользования.

Тармоқ маъмури томонидан, муҳофаза қилинадиган ресурсларнинг қиймати ва умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавфсизлигини таъминлаш тизимининг баҳосини ҳисобга олиб, тармоқнинг ахборот хавфсизлигига бўладиган маълум таҳдидларга қарши ҳаракат қилиш мақсадида ишлаб чиқилган, умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавфсизлиги объекти (объектлари) учун мўлжалланган талаблар ва қоидаларнинг жами.

1. Представление идентификации объекта или класса объектов и всех разрешенных видов доступа к этим объектам. Полномочие может быть реализовано в форме мандата.
2. Знак, используемый в качестве идентификатора для какого-либо ресурса, причем обладание таким знаком подтверждает право доступа к ресурсам.

1. Объектни ёки объектлар классини иден-

## П

тификация қилишни ва ушбу объектлардан эркин фойдаланишнинг барча рухсат этилган турларини тақдим этиш. Ваколат мандат шаклида амалга оширилиши мумкин.

2. Қандайдир ресурс учун идентификатор сифатида фойдаланиладиган белги. Бундай белгига эга бўлишлик ресурслардан фойдалана олиш ҳуқуқини тасдиқлайди.

### **Полубайт**

**uz** - ярим байт

**en** - nibble

Часть слова длиной в четыре бита.

Тўрт бит узунликдаги сўзнинг қисми.

### **Пользователь**

#### **авторизованный**

**uz** - муаллифлаштирилган фойдаланувчи

**en** - authorized user

Пользователь, наделенный определенными правами и привилегиями.

Маълум ҳуқуқ ва имтиёзларга эга фойдаланувчи.

#### **Пользователь зарегистрированный**

**uz** - рўйхатга олинган фойдаланувчи

**en** - registered user

1. Пользователь, имеющий приоритетный номер в данной системе коллективного пользования.

2. Пользователь, включенный в график работ на ЭВМ.

1. Берилган жамоа бўлиб фойдаланиш тизи мида устувор ракамга эга бўлган фойдаланувчи.

2. Электрон ҳисоблаш машинасидаги ишлар графигига киритилган фойдаланувчи.

#### **Пользователь (потребитель) информации**

**uz** - ахборотдан фойдаланувчи (ахборот истеъмолчиси)

**en** - information user

1. Субъект, обращающийся к информационным ресурсам за получением необходимой ему информации и пользующийся ею.

2. Юридическое или физическое лицо, обладающее полномочиями доступа к информации.

3. Субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установ-

## II

ленными правами и правилами доступа к информации либо с их нарушением.

1. Ахборот ресурсларига зарур ахборотни олиш ва ундан фойдаланиш учун мурожаат қилувчи субъект.

2. Ахборотдан фойдалана олиш ваколатига эга юридик ёки жисмоний шахс.

3. Ахборотдан эркин фойдаланишнинг белгиланган ҳуқуқ ва қоидаларига мувофиқ ёки уларни бузган ҳолда, ахборот эгаси ёки воситачисидан олинган ахборотдан фойдаланувчи субъект.

**Пользователь легальный**

**uz** - қонуний фойдаланувчи

**en** - legal user

Пользователь, имеющий законные основания для доступа к заданным ресурсам и сервисам.

Берилган ресурслар ва сервислардан эркин фойдаланиш учун қонуний асосга эга бўлган фойдаланувчи.

**Попытка доступа к информации неавторизованная**

**uz** - ахборотдан муаллифлаштирилмаган тарзда фойдаланишга уриниш  
**en** - hacking

Попытка получить доступ к информации за счет обхода (обмана) средств контроля доступа в сети.

Тармокдан эркин фойдаланишни назорат қилувчи воситаларни четлаб ўтиш (алдаш) ҳисобига ахборотдан фойдалана олишга уриниб кўриш.

**Попытка нарушения защиты прямая**

**uz** - муҳофазани бевоқифа бузишга уриниш  
**en** - direct attack

Попытка нарушения защиты системы, основанная на недостатках базовых алгоритмов, принципов или свойств механизма обеспечения безопасности.

Базавий алгоритмларнинг хавфсизликни таъминлаш механизми принциплари ёки ҳусусиятларининг камчиликларига асосланган, тизим муҳофазасини бузишга бўлган уриниш.

## П

### **Портал обеспечения безопасности кабельный**

**uz** - кабелли хавфсизликни таъминлаш портали  
**en** - cable security portal, CSP

### **Последовательность команд**

**uz** - командалар кетма-кетлиги  
**en** - command sequence

### **Последовательность сверхдлинная**

**uz** - ўта узун кетма-кетлик  
**en** - knapsack

### **Посредник**

**uz** - воситачи  
**en** - проху

Функциональный элемент, управляющий обеспечением безопасности и функциями преобразования между коаксиальным гибридным волоконным кабелем и домом.

Хавфсизлик таъминланишини ҳамда коаксиал гибрид толали кабель билан уй ўртасида ўзгартириш функцияларини бошқарувчи функционал элемент.

Совокупность команд или зарезервированных слов в программах на языке высокого уровня или множество кодов операций в программах на машинном языке.

Юқори даражали дастурлардаги командалар ёки резервланган сўзлар жами ёки машина тили дастурларидаги операцияларнинг кўшлаб кодлари (кодлар кўплиги).

Псевдослучайная последовательность с высокой криптостойкостью и сверхдлинным периодом повторения.

Юқори криптобардошлик ва ўта узун такрорланиш даврига эга псевдотасодифий кетма-кетлик.

Приложение, выполняемое на шлюзе, которое передает пакеты между авторизованным клиентом и внешним хостом. Посредник принимает запросы от клиента на определенные сервисы Internet, а затем, действуя от имени клиента (т.е. выступая его посредником), устанавливает соединения для полученного запрошенного сервиса. Все шлюзы прикладного уровня используют, связанные с приложениями, программы-посредники. Большинство шлюзов сеансового уровня-канальные посредники,

## II

которые обеспечивают те же функции перенаправления запросов, но поддерживают большую часть сервисов TCP/IP.

Шлюзда бажариладиган, муаллифлаштирилган мижоз ва ташки хост ўртасида пакетларни узатувчи илова (дастур). Воситачи Internet нинг маълум сервислари учун мижоздан сўров қабул қилади, кейин, мижоз номидан ҳаракат қилиб (яъни унинг воситачиси бўлиб), расмий равишда сўраб олинган сервис учун уланишни ўрнатади. Амалий даражадаги барча шлюзлар иловалар билан боғлиқ дастур-воситалардан фойдаланади. Сеанс даражасидаги кўпчилик шлюзлар сўровларни қайта йўналтиришнинг айнан бир хил функцияларини таъминлайдиган, лекин TCP/IP сервисларининг катта қисмини тутиб турадиган канал воситачиларидир.

**Потеря или искажение информации**

uz - ахборотнинг йўқотилиши ёки бузиб кўрсатилиши  
en - loss or corruption of information

Нарушение целостности переданных данных путем несанкционированного удаления, вставки, изменения порядка следования, повторного использования или задержки.

Рухсат этилмаган тарзда чиқариб ташлаш, киритиш, ўтиш тартибини ўзгартириш, такрор фойдаланиш ёки ушлаб қолиш йўли билан узатилган маълумотлар яхлитлигининг бузилиши.

**Поток ключевой**  
uz - калит оқими  
en - keystream

Длинная псевдослучайная последовательность, налагаемая на преобразуемое открытое сообщение с помощью побитового суммирования по модулю два.

Иккининг модули бўйича битма-бит жамлаш ёрдамида ўзгартириладиган очик ха-

## П

барга қўйиладиган узун псевдотасодифий кетма-кетлик.

### **Потоки информации**

**uz** - ахборот

оқимлари

**en** - information flow

Совокупность передаваемой информации между двумя и более взаимодействующими объектами.

Икки ва ундан ортиқ ўзаро ҳамкорлик қилувчи объект ўртасида узатиладиган ахборот жами.

### **Права пользователя**

**uz** - фойдаланувчи

нинг ҳуқуқи

**en** - user rights

Возможность произвести вход в систему определенного типа и наличие тех или иных привилегий.

Маълум турдаги тизимга киришни амалга ошириш имконияти ва у ёки бошқа имтиёзларнинг мавжудлиги.

### **Правила доступа**

**uz** - фойдалана

олиш қоидалари

**en** - access rule

1. Совокупность правил, регламентирующих порядок и условия доступа к защищаемой информации и ее носителям.

2. Правила, установленные для осуществления доступа субъекта к информационному ресурсу с использованием штатных технических средств.

1. Муҳофаза қилинадиган ахборот ва унинг ташувчиларидан фойдалана олиш тартиби ва шартларини қатъий тартибга соладиган қоидалар жами.

2. Штат техник воситаларидан фойдаланган ҳолда, субъектнинг ахборот ресурсидан фойдалана олишини амалга ошириш мақсадида ўрнатилган қоидалар.

### **Правила политики безопасности**

**uz** - хавфсизлик

сиёсати қоидалари

**en** - security policy

Местная информация, которая с учетом выбранных услуг безопасности определяет механизмы безопасности для применения, включая все параметры, необходимые для работы данного механизма.

## П

rules

Танлаб олинган хавфсизлик хизматларини ҳисобга олган ҳолда қўллаш учун хавфсизлик механизмларини, жумладан, ушбу механизмнинг ишлаши учун зарур бўлган барча параметрларни белгилайдиган маҳаллий ахборот.

**Право авторское**

**uz** - муаллифлик

ҳукуқи

**en** - copyright

Исключительное право, предоставляемое законом автору или его представителю, на воспроизведение, публикацию и копирование оригинальной работы.

Қонун томонидан муаллифга ёки унинг вакилига оригинал ишни қайта тиклаш, эълон қилиш ва нусха кўчириш учун тақдим этиладиган ягона ҳуқук.

**Право доступа**

**uz** - фойдалана

олиш ҳукуқи

**en** - access right

Совокупность правил доступа к защищаемой информации, установленных правовыми документами или собственником, владельцем информации.

Қонуний ҳужжатлар ёки ахборот эгаси, мулкдори томонидан белгиланган, муҳофазат қилинадиган ахборотдан фойдаланиш қоидаларининг жами.

**Право доступа к записи**

**uz** - ёзувдан фойдалана олиш ҳукуқи

**en** - write access control

Предоставление субъекту полномочий на запись (модификацию) определенной информации.

Субъектга маълум ахборотни ёзиш (ўзгартириш) учун ваколат бериш.

**Право доступа к чтению**

**uz** - ўқиш имкониятини олиш ҳукуқи

**en** - read access control

Предоставление субъекту полномочий на чтение определенной информации.

Субъектга маълум ахборотни ўқиш учун ваколат бериш.

## П

### **Предоставление права на доступ**

**uz** - фойдалана олиш ҳуқуқларини такдим этиш  
**en** - authorization

Выдача разрешения (санкции) на использование определенных программ и данных.

### **Предъявление пароля**

**uz** - паролни кўрсатиш  
**en** - sign-on

Муайян дастурлар ва маълумотлардан фойдаланишга рухсат (санкция) бериш.

Завершение идентификации и установления подлинности пользователя.

### **Преобразование информации криптографическое**

**uz** - ахборотни криптографик ўзгартириш  
**en** - cryptographic transformation of information

Идентификациялашнинг тугалланиши ва фойдаланувчининг ҳақиқийлигини ўрнатиш.

Процесс преобразования информации, основанный на применении криптографических методов (зашифрование и расшифрование, выработка и проверка электронной цифровой подписи, выработка и проверка хэш-функции).

### **Преобразования криптографические**

**uz** - криптографик ўзгартиришлар  
**en** - cryptographic transformation

Криптографик методларни (шифрлаш ва дастлабки матнга ўтириш электрон рақамли имзо ҳамда хэш-функцияни ишлаб чиқиш ва текшириш) кўллашга асосланган ахборотни ўзгартириш жараёни.

Совокупность операций шифрования и дешифрования данных, а также перешифрования данных при смене шифра.

### **Препятствие**

**uz** - тўсик  
**en** - interference

Маълумотларни шифрлаш ва дешифрлаш операцияларининг йиғиндиси, шунингдек, шифр алмашганда маълумотларни қайта шифрлаш.

Метод организационного, технического, программного преграждения доступа к защищаемой информации и объекту.

Мухофаза қилинадиган ахборот ва объектдан фойдалана олишга ташкилий, техник, дастурий жиҳатдан тўсқинлик қилиш методи.



## П

### **Прерывание**

**uz** - узилиш  
**en** - interrupt

Сигнал, по которому компьютер прекращает выполнение программы и начинает выполнять служебную программу.

### **Прерывание соединения**

**uz** - боғланишнинг узилиши  
**en** - connection interruption

Компьютер дастурнинг бажарилишини тўхтатадиган ва хизмат дастури бажарилишини бошлайдиган сигнал.

Разъединение, производимое в нарушение установленных процедур. Прерывание соединения может дать возможность другим логическим объектам получить несанкционированный доступ.

### **Преступление компьютерное**

**uz** - компьютер билан боғлиқ жиноят  
**en** - computer crime

Ўрнатилган процедураларни бузган ҳолда амалга ошириладиган узиб қўйиш. Боғланишнинг узилиши бошқа мантикий объектларга рухсат этилмаган тарзда фойдалана олиш имкониятини бериши мумкин.

Осуществление несанкционированного доступа к информационному ресурсу, его модификация (подделка) или уничтожение с целью получения имущественных выгод для себя или для третьего лица, а также для нанесения имущественного ущерба своему конкуренту.

Ахборот ресурсидан рухсат этилмаган тарзда фойдалана олиш, уни ўзгартириш (қалбакилаштириш) ёки ўзи учун ё учинчи шахс учун мулкий фойда олиш, шунингдек, ўз рақибига мулкий зарар етказиш максасида бу ресурсни йўқ қилиш.

**Привилегии**  
**uz** - имтиёзлар  
**en** - privileges

Право выполнять привилегированные, т.е. доступные ограниченному кругу пользователей запросы к операционной системе. Например, запрос на изменение системного времени.

## П

Операцион тизимга юборилган имтиёзли, яъни чекланган доирадаги фойдаланувчилар учун мумкин бўлган сўровларни бажа-риш хукуки. Масалан, тизим вақтини ўзгартиришга сўров.

**Пригодный/непригодный**

**uz** - яроқли/яроқсиз  
**en** - stun/unstun

Функция, позволяющая сделать украденную радиостанцию непригодной для использования злоумышленником.

Ўғирланган радиостанцияни жинояткор фойдаланиши учун яроқсиз ҳолатга келтириш имконини берувчи функция.

**Признак объекта демаскирующий косвенный**

**uz** - объектнинг демаскировкаловчи билвосита белгиси  
**en** - indirect unmask object characteristics

Технический демаскирующий признак, обусловленный действием обеспечивающих сил и средств или изменением окружающей среды в результате функционирования объекта защиты. К косвенным демаскирующим признакам относятся визуально-оптические признаки деятельности объекта, а так-же химическое или радиоактивное заражение местности.

Таъминловчи куч ва воситаларнинг ҳаракати ёки муҳофаза объектнинг ишлаши натижасида атроф-муҳитнинг ўзгариши билан боғлиқ демаскировкаловчи техник белги. Билвосита демаскировкаловчи белгиларга объект фаолиятининг визуал-оптик белгилари, шунингдек, жойнинг кимёвий ёки радиоактив зарарланиши киради.

**Принуждение**  
**uz** - мажбурлаш  
**en** - enforcement

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

## II

Муҳофаза методи, бунга кўра фойдаланувчилар ва тизим персонали моддий, маъмурий ёки жинойий жавобгарлик таҳдиди остида муҳофаза қилинадиган ахборотни қайта ишлаш, узатиш ва ундан фойдаланиш қоидаларига риоя қилишга мажбур бўладилар.

### Принцип Кирхгофа

uz - Кирхгоф принципи  
en - Kirchhoff principle

Принцип построения криптографических алгоритмов, согласно которому в секрете держится только определенный набор их параметров (ключ), а все остальное может быть открытым без снижения стойкости алгоритма ниже допустимой величины.

Криптографик алгоритмларни тузиш принципи. Унга кўра, бу алгоритмларнинг маълум бир тўплами (калит) сир тутилади, қолган барчаси эса алгоритм бардошлилигини йўл қўйиладиган микдордан пасайтирмасдан, очик бўлиши мумкин.

### Принцип «положено знать»

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

1. Обоснованное требование предполагаемого получателя ознакомиться с необходимыми данными, получить к ним доступ или овладеть любой чувствительной информацией, содержащейся в этих данных.
2. Необходимость иметь доступ, знать или обладать специальной информацией для выполнения своих служебных обязанностей.

1. Фараз қилинган олувчининг зарур маълумотлар билан танишиш, улардан эркин фойдаланишга рухсат олиш ёки ушбу маълумотлардаги исталган таъсирчан ахборотга эга бўлишнинг асосланган талаби.

2. Ўз хизмат вазифаларини бажариш учун махсус ахборотдан эркин фойдаланиш ҳуқуқига эга бўлиш, уни билиш ёки унга эгалик қилишнинг зарурлиги.

## II

**Принятие риска**  
**uz** - риск (эхтимолий хавф)ни қабул қилиш  
**en** - risk acceptance

**Проверка безопасности**  
**uz** - хавфсизликни текшириш  
**en** - security inspection

**Проверка достоверности данных**  
**uz** - маълумотларнинг ишончлилигини текшириш  
**en** - data validation

Идентификация и принятие риска, связанного с исключительной ситуацией в политике безопасности.  
Хавфсизлик сиёсатидаги фавқуллодда вазият билан боғлиқ, риск (эхтимолий хавф)ни идентификациялаш ва қабул қилиш.

Независимый просмотр, изучение системных журналов и наблюдение за функционированием с целью определения достаточности средств контроля системы, соответствия принятой политике безопасности и процедурам обработки данных, обнаружения нарушений безопасности, выработки рекомендаций по изменению средств контроля и процедур безопасности.

Тизимни назорат қилиш воситаларининг етарлилигини, қабул қилинган хавфсизлик сиёсатида ва маълумотларни қайта ишлаш процедураларига мослигини, хавфсизлик бузилишларини аниқлаш, назорат воситалари ва хавфсизлик процедураларини ўзгартириш бўйича тавсиялар ишлаб чиқиш мақсадида тизим журналларини мустақил кўриб чиқиш, ўрганиш ва ишлаши устидан кузатиш олиб бориш.

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.*

Маълумотларнинг аниқлигини, уларнинг тўлиқлигини ёки берилган критерийларга мослигини аниқлаш учун қўлланиладиган жараён.

*Изоҳ: Маълумотларнинг ишончлилигини текши-*

## П

*риш уларнинг форматларини ва тўлиқлигини текшириш, калитнинг назорат тестлари, тўзри-лигини ва чеклашларни текширишдан иборат.*

### **Проверка криптографическая**

**uz** - криптографик текширув  
**en** - cryptographic verification

Процесс извлечения информации с помощью криптографического преобразования.

Криптографик ўзгартириш ёрдамида ахборот олиш жараёни.

### **Проверка ограничения**

**uz** - чеклашни текшириш  
**en** - limit check

Проверка, выполняемая, чтобы определить, находятся ли значения данных выше или ниже заданного значения или достигли установленного ограничения.

Маълумотларнинг қийматлари берилган қийматдан юкорида ёки куйида турганлигини ёки белгиланган чеклашга етганлигини аниқлаш мақсадида бажариладиган текшириш.

### **Проверка подлинности**

**uz** - ҳақиқийликни текшириш  
**en** - authentication

Процедура, удостоверяющая, что пользователь именно тот, за кого себя выдает. В простейшем случае проверяется знание пользователем пароля, хранящегося в его учетной записи.

Фойдаланувчининг, ўзини айнан шу одам деб кўрсатишлигини тасдиқловчи процедура. Оддий ҳолда фойдаланувчининг, унинг ҳисобга олиш ёзувида сақланадиган, паролни билиши текширилади.

### **Проверка подлинности сквозная**

**uz** - ҳақиқийликни ялпи текшириш  
**en** - throughout authentication

Проверка подлинности, при которой компьютер входа передает сведения, идентифицирующие пользователя, на другой компьютер.

Ҳақиқийликни текшириш, бунда кириш компютери фойдаланувчини идентификация қилувчи ахборотни бошқа Компьютерга узади.

## П

**Проверка правильности (данных) на входе**

**uz** – киришда (маълумотларнинг) тўғрилигини текшириш  
**en** - input (data) validation

Процесс, используемый, чтобы определить неточность данных на входе, их незавершенность или нелогичность.

Маълумотларнинг киришда ноаниқлигини, уларнинг тугалланмай қолганлигини ёки мантиқий эмаслигини аниқлаш мақсадида фойдаланиладиган жараён.

**Проверка системы**

**uz** - тизимни текшириш  
**en** - system checkout

Исследование процедур, используемых в системе, чтобы оценить их эффективность и правильность, а также рекомендовать усовершенствования.

Тизимда фойдаланиладиган процедураларни, уларнинг самарадорлигини ва тўғрилигини баҳолаш, шунингдек, такомиллаштиришни тавсия этиш мақсадида ўрганиш.

**Проверка специальная**

**uz** - махсус текширув  
**en** - special checkout

Проверка технического средства обработки информации, осуществляемая с целью поиска и изъятия специальных электронных закладных устройств (аппаратных закладок).

Ахборотни қайта ишлаш техник воситасини текшириш. Махсус (яширин) урнатиладиган электрон қурилмаларни (аппарат қўйилмаларни) кидириб топиш ва олиб қўйиш мақсадида амалга оширилади.

**Проверка формата**

**uz** - форматни текшириш  
**en** - format check

Проверка, выполняемая, чтобы определить, соответствуют ли данные определенному шаблону.

Маълумотлар маълум бир намунага мос келишини аниқлаш мақсадида амалга ошириладиган текширув

**Программа**

**uz** - дастур

Последовательность операторов, предназначенных для реализации на ЭВМ.

## II

en - program, programme

Электрон ҳисоблаш машинаси (ЭХМ)да амалга ошириш учун мўлжалланган операторлар кетма-кетлиги.

**Программа анти-вирусная**

uz - вирусга қарши дастур

en - anti-virus program

Программа, предназначенная для обнаружения вирусов и, возможно, предлагающая удалить или удаляющая их.

**Программа-вакцина**

uz - вакцина-дастур  
en - vaccine program

Программа, которая модифицирует другие программы и диски таким образом, что это не отражается на их работе, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными.

Бошқа дастурлар ва дискларни уларнинг ишига таъсир қилмайдиган даражада ўзгартирадиган дастур. Бироқ вакцинация манбаи бўлган вирус бу дастурлар ёки дисклар зарарланиб бўлган деб ҳисоблайди.

**Программа вредоносная**

uz - зарарловчи дастур

en - malicious program

Программа, реализованная аппаратным, программно-аппаратным или программным способом и предназначенная для выполнения каких-либо несанкционированных или злоумышленных действий. Например, логическая бомба, троянский конь, вирус, червь.

Аппарат, дастурий-аппарат ёки дастурий усулда амалга оширилган ва бирор-бир рухсат этилмаган ёки жинояткорона ҳаракатларни бажариш учун мўлжалланган дастур. Масалан, мантиқий бомба, троя оти, вирус, курт.

**Программа диагностическая**

uz - диагностик дастур

1. Программа запуска тестов для выявления возможных и реальных неисправностей в системе.

2. Программа, предназначенная для обна-

## II

**en** - diagnostic routine

ружения, локализации и описания неисправностей технического оборудования или ошибок программ.

1. Тизимдаги мумкин бўлган ва реал носозликларни аниқлаш учун тестларни ишга тушириш дастури.

2. Техник ускуна носозликларини ёки дастурдаги хатоликларни аниқлаш, бартараф этиш ва тавсифлаш учун мўлжалланган дастур.

**Программа само-загрузки**

**uz** - ўз-ўзидан юклаш дастури  
**en** - bootstrap

Минимальное множество команд, необходимое для загрузки операционной системы.

Операцион тизимни юклаш учун зарур бўлган командаларнинг минимал кўплиги.

**Программа TEMPEST**

**uz** - TEMPEST дастури  
**en** - TEMPEST program

Программа изучения и анализа побочных электромагнитных сигналов, излучаемых электрическим и электронным оборудованием.

Электр ва электрон ускуна нурлантирадиган кўшимча электромагнит сигналларни ўрганиш ва таҳлил қилиш дастури.

**Программы бесплатные**

**uz** - бепул дастурлар  
**en** - freeware

Распространяемые бесплатно программы. Бесплатные программы не эквивалентны общедоступным программам, так как их разработчик сохраняет авторское право.

Бепул тарқатиладиган дастурлар. Бепул дастурлар, уларни ишлаб чиқувчи муаллифлик ҳуқуқини сақлаб қолганлиги тўғрисида, умумқойдаланиш дастурларига эквивалент бўлмайд.

**Программы-детекторы**

**uz** - детектор дастури

Программы, позволяющие обнаруживать файлы, зараженные одним из нескольких известных вирусов. Многие из этих про-



## II

турлар  
en - detector  
software

грамм имеют режимы лечения или уничтожения зараженных файлов.

Маълум бўлган бир қанча вирусларнинг бири билан зарарланган файлларни аниқлаш имкони берадиган дастурлар. Бу дастурлардан кўпчилиги зарарланган файлларни тузатиш ёки йўқ қилиш режимларига эга.

**Программы**  
**доктора-ревизоры**  
uz - доктор-ревизор  
дастурлар  
en - doctor-inspector  
program

Программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние.

Файллардаги ва дискларнинг тизим соҳаларидаги ўзгаришларни аниқлабгина қолмай, балки ўзгаришлар юз берганда уларни дастлабки ҳолатга автоматик равишда қайтаридиган дастурлар.

**Программы обще-**  
**доступные**  
uz - умумфойдаланиш  
дастурлари  
en - common access  
software

Программы, которые распространяются и используются бесплатно.

Беғул тарқатиладиган ва фойдаланиладиган дастурлар.

**Программы-**  
**ревизоры**  
uz - ревизор дастурлар  
en - inspector  
programs

Программы, с помощью которых можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

Шундай дастурларки, уларнинг ёрдамида дастурларнинг ва дисклар тизим соҳаларининг ҳолатини дастлабки ҳолат билан такқослаш мумкин. Аниқланган номувофикликлар тўғрисида фойдаланувчига хабар қилинади.

## II

### **Программы-фильтры**

**uz** - филтр дастурлар  
**en** - filter programs

Программы, располагающиеся резидентно в оперативной памяти компьютера и перехватывающие те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, а также сообщающие о них пользователям.

Компьютернинг оператив хотирасида резидент тарзда жойлашган ва операцион тизимга қилинган, вируслар кўпайиш ва зарар етказиш учун фойдаланадиган муружаатларни тутиб оладиган, шунингдек, улар тўғрисида фойдаланувчига хабар берадиган дастурлар.

**Продажа вызовов**  
**uz** - чакирувларни сотиш  
**en** - call selling

Вид криминальной деятельности, при котором злоумышленник получает прибыль, продавая дорогостоящие вызовы со значительными скидками, используя одну или несколько линий телекоммуникаций с максимальной загрузкой, организуя нелегальные «телефонные переговорные пункты».

Жиноий фаолият тури, бунда жинояткор максимал юкланишдаги бир ёки бир нечта телекоммуникациялар линиясидан фойдаланган ҳолда яширин «телефон сўзлашув пунктлари»ни ташкил қилиб, баланд нархли чакирувларни катта чегирма билан сотиб, фойда олади.

**Проникновение**  
**uz** - сукулиб кириш  
**en** - penetration

1. Успешное преодоление механизмов защиты системы.  
2. Несанкционированный доступ к системе обработки данных.

1. Тизимнинг муҳофаза қилиш механизмларини муваффақиятли енгиб ўтиш.  
2. Маълумотларни қайта ишлаш тизимига рухсат этилмаган тарзда кириш.

## П

**Прослушивание**  
**uz** - эшитиш  
**en** - eavesdropping

Несанкционированный перехват информационных излучений.

Ахборот нурланишларини рухсат этилмаган тарзда тутиб олиш.

**Просмотр**  
**uz** - кўриб чиқиш  
**en** - browsing

Поиск информации, нередко преследующий цель получения несанкционированного доступа к конфиденциальным данным и представляющий в этом случае угрозу для системы.

Ахборот излаш бўлиб, кўпинча конфиденциал маълумотлардан рухсат этилмаган тарзда фойдаланишни мақсад қилиб қўяди, шу туфайли тизим учун хавф туғдиради.

**Противодействие сетевым угрозам**  
**uz** - тармоқ тахдидларига қарши туриш  
**en** - network threat counteraction

Комплекс мер безопасности, предназначенный для защиты сетевой инфраструктуры от атак злоумышленников.

Тармоқ инфраструктурасини жинояткорларнинг хужумларидан муҳофаза қилиш учун мўлжалланган хавфсизлик чоралари комплекси.

**Протокол безопасной передачи данных**  
**uz** - маълумотларни хавфсиз узатиш протоколи  
**en** - secure sockets layer, SSL

Протокол, используемый для окончного шифрования трафика на прикладном уровне.

Амалий даражада трафикни охирги шифрлаш учун фойдаланиладиган протокол.

**Протокол криптографический**  
**uz** - криптографик протокол  
**en** - cryptographic protocol

1. Алгоритм, посредством которого две или более стороны обмениваются некоторой информацией и который гарантирует безопасность обмениваемой информации. Такой алгоритм использует криптографические преобразования и обычно базируется на криптографии с открытыми ключами.

## II

2. Набор правил и процедур, определяющих использование криптоалгоритма и ключей шифрования.

3. Протокол, предусматривающий взаимодействие двух и более сторон с использованием криптографических алгоритмов.

1. Алгоритм, унинг воситасида икки ёки ундан ортик томон кандайдир ахборотни алмашинади ва алмашинадиган ахборотнинг хавфсизлиги кафолатланади. Бундай алгоритм криптографик ўзгартиришлардан фойдаланади ва одатда, очик калитли криптографияга асосланади.

2. Криптоалгоритмдан ва шифрлаш калитларидан фойдаланишни белгилайдиган қондалар ва процедуралар тўплами.

3. Криптографик алгоритмлардан фойдаланган ҳолда икки ва ундан кўп томоннинг ўзаро ишлашнинг кўзда тутовчи протокол.

### Протокол отрицания

uz - инкор қилиш протоколи  
en - denial protocol

Тип протокола, не позволяющий подписывающему лицу отказаться от подписанного сообщения.

Имзо чекувчи шахсга имзоланган хабарни рад қилишига йўл қўймайдиган протокол тури.

### Протокол распределения ключей

uz - калитларни тақсимлаш протоколи  
en - key distribution protocol

Протокол, в результате выполнения которого взаимодействующие стороны (пользователи, группы пользователей) получают необходимые для функционирования криптографической системы ключи.

Бажарилиши натижасида биргаликда ишлайдиган томонлар (фойдаланувчилар, фойдаланувчилар гуруҳи) криптографик тизим ишлаши учун зарур бўлган калитларни оладиган протокол.

## II

**Протокол с арбитром**

**uz** - арбитрли протокол

**en** - protocol with arbiter

Криптографический протокол, в котором используется одна или несколько незаинтересованных доверенных сторон (арбитров). Доверенность означает, что все участники протокола признают, что любые утверждения или действия арбитра истинны и корректны.

Бир ёки бир нечта манфаатдор бўлмаган ваколатли томонлар (атрибутилар) дан фойдаланиладиган криптографик протокол. Ваколатнома протоколнинг барча иштирокчилари арбитраж ҳар қандай тасдиқлаши ёки ҳаракатлари тўғри ва ҳақиқий эканлигини тан олишларини билдиради.

**Протокол с третейским судьей**

**uz** - манфаатдор бўлмаган

ҳакам протоколи

**en** - protocol with arbitrator

Протокол, аналогичный протоколу с арбитром, но в отличие от последнего, третейский судья появляется только в случае возникновения спорных ситуаций между участниками протокола. Третейский судья, в отличие от арбитра, не участвует напрямую в протоколе, однако существуют данные, которые позволяют третейскому судье определить обман.

Арбитраж протоколга ўхшаш протокол, лекин ундан фаркли равишда манфаатдор бўлмаган ҳакам фақат протокол иштирокчилари ўртасида баҳсли ҳолатлар юз берган ҳоллардагина пайдо бўлади. Манфаатдор бўлмаган ҳакам, арбитраждан фаркли равишда, тўғридан-тўғри протоколда иштирок этмайди, лекин манфаатдор бўлмаган ҳакамга алдовни аниқлаш учун имкон берадиган маълумотлар мавжуд бўлади.

**Протокол, самообеспечивающий законность**

Один из лучших типов криптографических протоколов, позволяющих обойтись без третьей стороны. В данном типе протокола

## II

**uz** - қонунийликни ўзи таъминлайдиган протокол  
**en** - self maintain law protocol

он сам гарантирует соблюдение всех правил. Такой протокол построен так, что в случае возникновения обмана с одной стороны, другая сторона всегда может определить это.

Криптографик протоколларнинг учинчи томонга эҳтиёж бўлмаган энг яхши турларидан бири. Протокол барча қоидаларга риоя қилинишини кафолатлайди. Бундай протокол бир томонда алдов пайдо бўлганда бошқа томон ҳар доим буни аниқлаши мумкин бўлган тарзда тузилган.

**Протоколы**  
**uz** - протоколлар  
**en** - protocols

1. Набор правил и форматов, семантических и синтаксических, позволяющих различным компонентам системы обмениваться информацией (например, узлам сети).
2. Согласованные процедуры передачи данных между различными объектами вычислительной системы.

1. Тизимнинг турли компонентларига (масалан, тармок узелларига) ахборот алмашиниши учун имкон берувчи семантик ва синтаксик қоидалар, форматлар тўплами.
2. Ҳисоблаш тизимининг турли объектлари ўртасида маълумотлар узатишнинг келишилган процедуралари.

**Профиль защиты**  
**uz** - муҳофаза профили  
**en** - protection profile

1. Не зависящая от реализации (не связанная с реализацией) совокупность требований безопасности для некоторой категории объектов оценки, отвечающей специфическим потребностям потребителя.
2. Функционально полный, прошедший апробацию, стандартизированный набор требований, предназначенный для многократного использования.

## II

1. Амалга ошириш билан боғлиқ бўлмаган, истемолчининг специфик эҳтиёжларига жавоб берадиган, қандайдир категориядаги баҳолаш объектлари учун мўлжалланган хавфсизлик талабларининг жами.

2. Функционал жиҳатдан тўла, апробациядан ўтган, кўп маротаба фойдаланиш учун мўлжалланган, стандартлаштирилган талаблар тўплами.

### **Профиль полномочий**

**uz** - ваколатлар профили  
**en** - authorized profile

Список защищаемых объектов системы и прав доступа к ним, ассоциированный с каждым субъектом. При обращении к объекту профиль субъекта проверяется на наличие соответствующих прав доступа. Профиль представляется в виде строки матрицы доступа.

Ҳар бир субъект билан ассоциацияланган тизимнинг муҳофаза қилинадиган объектлари ва улардан эрин фойдаланиш ҳуқуқлари рўйхати. Объектга мурожаат қилишда субъект профили фойдаланишнинг тегишли ҳуқуқлари мавжудлигига текширилади. Профиль эркин фойдаланиш матрицасининг сатри кўринишида тақдим этилади.

### **Профиль пользователя**

**uz** - фойдаланувчининг профили  
**en** - user profile

1. Описание пользователя, обычно используемое для управления доступом.

*Примечание: Профиль пользователя может содержать такие данные как идентификатор пользователя, имя пользователя, пароль, права на доступ и другие атрибуты.*

2. Образец деятельности пользователя, который может использоваться для обнаружения изменений в его деятельности.

1. Одатда, эркин фойдаланишни бошқариш учун қўлланиладиган фойдаланувчининг тавсифи.

*Изоҳ: Фойдаланувчининг профили фойдаланувчининг идентификатори, фойдаланувчининг но-*

## П

*ми, пароль, эркин фойдаланиш ҳуқуқи ва бошқа атрибутлардан иборат бўлиши мумкин.*

2. Фойдаланувчи фаолиятининг намунаси фойдаланувчининг фаолиятидаги ўзгаришларни аниқлаш учун қўлланилади.

**Проход через систему защиты, обходной путь**

**uz** - муҳофаза тизими орқали ўтиш, айланма йўл  
**en** - security trap-door, bypass path

Блок обхода, встроенный в систему шифрования.

Шифрлаш тизимида киритилган четлаб ўтиш блоки.

**Процедура резервирования**

**uz** - резервлаш процедураси  
**en** - backup procedure

Процедура, предусматривающая реставрацию данных после сбоя или аварии. Например, создание резервных файлов.

Тўхтаб қолиш ёки авариядан кейин маълумотларнинг қайта тикланишини кўзда тутовчи процедура. Масалан, резерв файлларни яратиш.

**Процедуры восстановительные**

**uz** - тикловчи процедуралар  
**en** - recovery procedures

Действия, предпринимаемые для восстановления способности системы обрабатывать информацию, а также восстановления наборов данных после аварии или сбоя.

Тизимнинг ахборотни қайта ишлаш қобилиятини тиклаш учун қилинадиган ҳаракатлар, шунингдек, авария ёки тўхтаб қолишдан сўнг маълумотлар тўпламларини тиклаш.

**Процесс**

**uz** - жараён  
**en** - process

1. Объект операционной системы, включающий, помимо прочего, защищенную область памяти с исполняемым кодом и данными, один или несколько потоков исполнения и главный маркер доступа.

2. Выполняющаяся программа.



## II

1. Хотиранинг бажарилувчи кодлар ва маълумотлар билан муҳофазаланган соҳасини, бир ёки бир нечта бажариш оқимини ҳамда фойдаланишнинг бош маркерини ўз ичига олувчи операцион тизим объекти.

2. Бажарилаётган дастур.

**Процессы информации**

**uz** - ахборот жараёнлари

**en** - informational process

Процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Ахборотни йиғиш, қайта ишлаш, тўплаш, сақлаш, излаш ва тарқатиш жараёнлари.

**Прошивка сети**

**uz** - тармоқдан кибриб олиш

**en** - network weaving

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

Сукулиб кириш усули, бунда маълумотларни қайта ишлаш тизимига кира олиш йўлини топиш мақсадида телекоммуникацияларнинг турли тармоқларидан фойдаланилади, жойлашган ўрин аниқланиши мумкин бўлган ҳолларнинг олди олинади.

**Пункт обработки данных запасной**

**uz** - маълумотларни қайта ишлаш захира пункти

**en** - cold site

Возможно минимальное количество оборудования, необходимого для инсталляции и задействования резервной системы обработки данных.

Инсталляция ва маълумотларни қайта ишлаш резерв тизими ишга туширилиши учун зарур ускунанинг мумкин бўлган минимал микдори.

**Пункт обработки данных резервный**

**uz** - маълумотларни қайта ишлаш резерв

Полностью оборудованный вычислительный центр, который обеспечивает возможность немедленной альтернативной обработки данных.

## П

пункти  
en - hot site

Маълумотларни зудлик билан муқобил қайта ишлаш имконини берувчи, тўлик жиҳозланган ҳисоблаш маркази.

**Путь доступа**  
uz - кира олиш  
(фойдалана олиш)  
йўли  
en - access path

Последовательность элементов данных, которые используются системой управления базой данных для доступа к записям или другим элементам данных, хранящимся в базе данных.

**Путь обхода системы защиты**  
uz - муҳофаза қилиш тизимини четлаб ўтиш йўли  
en - trapdoor

Маълумотлар элементларининг кетма-кетлиги, улар маълумотлар базасини бошқариш тизими томонидан ёзувлардан ёки маълумотлар базасида сақланадиган маълумотларнинг бошқа элементларидан эркин фойдаланишда қўлланилади.

Результат действия, при котором объект системы претерпевает изменение, для того чтобы позволить злоумышленнику оказать несанкционированное влияние на команду или на predetermined событие или на последовательность событий. Например, проверка пароля может быть изменена таким образом, что, помимо своего обычного результата она, подтверждает также правильность пароля злоумышленника.

**Путь проникновения**

Ҳаракат натижаси бўлиб, бунда тизим объекти жинояткорга командага ёки олдиндан белгиланган воқеага ёки воқеалар кетма-кетлигига руҳсат этилмаган тарзда таъсир кўрсатиш имконини берадиган даражада ўзгаради. Масалан, паролни текшириш шундай ўзгартирилиши мумкинки, у одатдаги ўзининг натижасидан ташқари, жинояткор паролининг тўғрилигини ҳам тасдиқлайди.

Последовательность несанкционированных действий пользователя при его проникно-

## П

**uz** - сукулиб кириш  
йўли  
**en** - penetration  
route

вении в защищенную систему.  
Муҳофазаланган тизимга сукулиб кириш пайтида фойдаланувчи рухсат этилмаган ҳаракатларининг кетма-кетлиги.

**Путь сертификата**  
**uz** - сертификат  
йўли  
**en** - certification  
path

Упорядоченная последовательность сертификатов объектов в информационном дереве каталога, которая вместе с открытым ключом первоначального объекта данного пути может быть обработана для получения открытого ключа конечного объекта данного пути.

Объектлар сертификатларининг, каталогнинг ахборот дарахтидаги тартиблаштирилган кетма-кетлиги бўлиб, берилган йўл бошланғич объектнинг очик калити билан бирга шу йўл охириги объектнинг очик калитини олиш мақсадида қайта ишланиши мумкин.

**«Пятна родимые»**  
**uz** - «хол»  
**en** - birthmarks

Присущие автору в процессе написания программы особенности стиля: типичные ошибки, избыточные данные и характерные черты программирования, позволяющие выявить очевидность заимствования.

Дастурни ёзиш жараёнида муаллифга хос услубнинг хоссаси: типик хатолар, ўзлаштирманинг аёнлигини аниқлашга имкон берувчи ортиқча маълумотлар ва дастурлашдаги характерли хусусиятлар.

## Р

**Работа секретная**  
**uz** - махфий иш  
**en** - secret work

Научно-исследовательские, опытно-конструкторские, проектные, технологические, изыскательские и иные работы (в том числе работы студентов, дипломников, диссертантов), а также любые сведения, преду-

## Р

смотренные в Перечне сведений, подлежащих засекречиванию

Илмий-тадқиқот, тажриба-конструкторлик, лойиҳа, технологик, қидирув ва бошқа ишлар (шу жумладан, талабалар, дипломниклар, диссертантларнинг ишлари), шунингдек, махфийлаштириш лозим бўлган маълумотлар рўйхатида кўзда тутилган ҳар қандай маълумот.

### **Работоспособность сети**

**uz** - тармоқнинг иш қобилияти

**en** - network capability

Свойство сети выполнять заданные функции в соответствии с установленными требованиями.

Тармоқнинг берилган функцияларни белгиланган талабларга мувофиқ бажариш хусусияти.

### **Радиокиллер**

**uz** - радиокиллер

**en** - radio killer

Специальная команда, переданная оператором транкинговой сети на абонентскую станцию (обычно похищенную) и вызывающая в ней необратимые изменения, делающие ее непригодной к работе.

Транкинг тармоқ оператори томонидан абонент станциясига (одатда, ўғирланган) узатилган ва унда, уни ишга яроқсиз қилувчи, қайтариб бўлмайдиган ўзгаришлар пайдо қиладиган махсус команда.

### **Радиус (опасной) зоны**

**uz** - (хавфли) зона радиуси

**en** - dangerous area radius

Радиус сферы, охватывающий зону 1 или зону 2.

1- ёки 2- зонани қамраб олувчи сфера радиуси.

### **Развертывание ключа**

**uz** - қалитни очиб

Процедура выработки последовательности раундовых ключей из ключа шифрования. Обычно суммарный объем раундовых ключей

## Р

кўрсатиш  
en - key scheduling

чей значительно превышает размер ключа шифрования.

Шифрлаш калитидан раундли калитлар кетма-кетлигини ишлаб чиқиш процедура-си. Одатда, раундли калитларнинг жами ҳажми шифрлаш калитининг ўлчамидан анча кўп бўлади.

**Разглашение ин-  
формации**  
uz - ахборотнинг  
ошкор бўлиши  
en - information  
disclosure

Несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к защищаемой информации.

Муҳофаза қилинадиган ахборотнинг бундай ахборотдан эркин фойдаланиш ҳуқуқи бўлмаган истеъмолчиларга руҳсат этилмаган тарзда етказилиши.

**Разграничение  
доступа**  
uz - эркин фойда-  
ланишни чегаралаш  
en - access isolation

1. Порядок использования ресурсов системы, при котором субъекты получают доступ к объектам в строгом соответствии с установленными правилами.

2. Наделение каждого пользователя (субъекта доступа) индивидуальными правами по доступу к информационному ресурсу и проведению операций по ознакомлению с информацией, ее документированию, модификации и уничтожению.

*Примечание: Разграничение доступа может осуществляться по различным моделям, построенным по тематическому признаку или по грифу секретности разрешенной к пользованию информации.*

1. Тизим ресурсларидан фойдаланиш тартиби, бунда субъектлар белгиланган қоидаларга қатъий мувофиқ ҳолда объектлардан фойдалана оладилар.

2. Ҳар бир фойдаланувчига (фойдаланиш субъектига) ахборот ресурслардан эркин фойдаланиш, ахборот билан танишиш, уни

## Р

хужжатлаштириш, ўзгартириш ва йўқ қилиш бўйича операцияларни амалга ошириш юзасидан алоҳида ҳуқуқлар бериш.

*Изоҳ: Эркин фойдаланишни белгилаш тематик белгига кўра қурилган турли моделлар ёки фойдаланиш руҳсат этилган ахборотнинг махфийлик грифи бўйича амалга оширилиши мумкин.*

### Разграничение обязанностей

**uz** - мажбуриятларнинг аниқ белгилаб олинishi  
**en** - separation of duties

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

Таъсирчан ахборотга нисбатан жавобгарликнинг бўлиниши, бу жараён шундай тарзда бажариладики, бунда бир ўзи ҳаракат қилаётган шахс маълумотларни қайта ишлаш тизими чекланган қисмининггина хавфсизлигига путур етказиши (хавфсизлигини обрўсизлантириши) мумкин.

**Разделение**  
**uz** - ажратиш  
**en** - division

Деление данных на изолированные блоки, управление безопасностью которых производится отдельно, с целью уменьшения риска. Например, чтобы ограничить воздействие на весь проект производится разделение данных главного проекта на блоки, соответствующие разделам проекта, каждый из которых имеет собственную систему безопасности.

Маълумотларни изоляцияланган блокларга бўлиш. Риск (эхтимолий хавф)ни камайтириш мақсадида уларнинг хавфсизлигини бошқариш алоҳида амалга оширилади. Масалан, бутун лойиҳага таъсирни чеклаш учун бош лойиҳа маълумотлари лойиҳанинг ўз хавфсизлик тизимига эга бўлган,

## Р

ҳар бир тегишли бўлимига мос келадиган блоklarга ажратилади.

### Разделение привилегий

**uz** - имтиёзларнинг тақсимланиши  
**en** - privilege sharing

Принцип открытия механизма защиты данных, при котором для доступа к ним необходимо указать не один, а два пароля (например, двумя лицами).

Маълумотларни муҳофаза қилиш механизмини очиш принципи, бунда эркин фойдаланиш (кириш) учун бир эмас, балки иккита паролни (масалан, иккита шахс томонидан) кўрсатиш зарур бўлади.

### Разделение секретов

**uz** - сирларнинг тақсимланиши  
**en** - secret sharing scheme

Схема разделения секрета, основная идея которой – разделить секретный ключ между несколькими субъектами, чтобы собравшись вместе они могли восстановить ключ из нескольких частей.

Сирни тақсимлаш схемаси, унинг асосий ғояси махфий калитни бир нечта субъект ўртасида, улар бирга тўпланиб, калитни бир нечта қисмлардан тиклашлари мумкин бўладиган тарзда ажратишда ифодаланади.

### Разметка дорожек спиральной

**uz** - йўлкаларни спираль бўйича белгилаб чиқиш  
**en** - spiral tracking

Метод защиты от копирования, в котором используется для чтения данных только часть каждой дорожки, при этом головка, читающая содержимое диска, будет двигаться к центру приблизительно по спирали.

Нусха кўчиришдан муҳофаза қилиш методи, унда маълумотларни ўқиш учун ҳар бир йўлқанинг фақат бир қисмидан фойдаланилади, бунда диск ичидагиларни ўқувчи каллак марказга тахминан спираль бўйича ҳаракат қилади.

### Разметка ложная

**uz** - чалғитувчи

Способ защиты от копирования, при использовании которого на диске специально

## Р

белги  
en - bad tracking

записываются дефектные секторы.

**Разрешение**  
uz - рухсат  
en - permission

Нусха кўчиришдан муҳофаза қилиш методи, ундан фойдаланилганда дискда нуксонли секторлар махсус ёзиб олинади.

Набор типов доступа, используемый в административных программах при формировании списков контроля доступа.

**Разрешение на доступ**  
uz - эркин фойдаланишга рухсат  
en - access permission

Эркин фойдаланиш турлари тўплами эркин фойдаланишни назорат қилиш рўйхатини шакллантиришда маъмурий дастурларда қўлланилади.

Все права на доступ субъекта к некоторому объекту.

**Разрушение информации**  
uz - ахборотнинг бузилиши  
en - information destruction

Субъектнинг қандайдир объектдан эркин фойдаланишини таъминлайдиган барча хуқуқлар.

1. Любое состояние данных независимо от причины, которое делает невозможным использование информации.

2. Стирание информации, хранящейся в памяти ЭВМ.

**Разрушение секретной информации**  
uz - махфий ахборотнинг бузилиши  
en - secret nforma-

1. Қандай сабаб бўлишидан қатъи назар, маълумотларнинг, ахборотдан фойдаланиш имкониятини йўққа чиқарадиган, ҳар қандай ҳолати.

2. Электрон ҳисоблаш машинаси хотирасида сақланадиган ахборотнинг ўчириб юборилиши.

Неправомерное или преднамеренное изменение, искажение или уничтожение информации в результате неисправности технических средств, несовершенства и ошибок программного обеспечения, халатности обслуживающего персонала, стихийных



## Р

tion destruction

бедствий или действий злоумышленников (нарушителей).

Техник воситаларнинг носозлиги, дастурий таъминотнинг такомиллашмаганлиги ва хатолари, хизмат кўрсатувчи персоналнинг масъулиятсизлиги, табиий офатлар ёки жинояткорлар (бузғунчилар) ҳаракатлари натижасида ахборотнинг ноқонуний ёки қасддан ўзгартирилиши, бузилиши ёки йўқ қилиниши.

### Разрыв линии

uz - линиянинг узилиши

en - line disconnect

Метод проведения атаки на систему, при котором пользователь выходит из системы либо злоумышленник разрывает линию телекоммуникаций, но система продолжает работу с злоумышленником как с легальным пользователем.

Тизимга қилинадиган хужумни амалга ошириш методи, бунда фойдаланувчи тизимдан чиқади ёки жинояткор телекоммуникациялар линиясини узиб қўяди, бироқ тизим жинояткор билан очик фойдаланувчи билан бўлганидек ишлашни давом эттираверади.

### Разряд защиты

uz - муҳофаза разряди

en - protection bit

Один из дополнительных разрядов промежуточных результатов, обеспечивающих сохранение точности.

Аниқлик сақланиб қолишини таъминлайдиган оралик натижаларнинг қўшимча разрядларидан бири.

### Рандомизация

uz - рандомизация(лаш)

en - randomisation

Преобразование исходных данных перед или во время зашифрования с использованием псевдослучайной последовательности данных, имеющее целью скрыть наличие в них, например, идентичных блоков.

## Р

Маълумотларда идентик блоклар мавжудлигини яшириш мақсадида, маълумотларнинг псевдотасодифий кетма-кетлигидан фойдаланиб, шифрлашдан олдин ёки шифрлаш пайтида бошланғич маълумотларни ўзгартириш.

### Раскрытие

**uz** - очилиш (фош этилиш)

**en** - disclosure, reveal

Операция частичного или полного удаления ранее примененной защиты.

Илгари қўлланилган муҳофазани қисман ёки тўлиқ олиб ташлаш операцияси.

### Раскрытие информации

**uz** - ахборотнинг фош этилиши

**en** - disclosure of information

1. Нарушение компьютерной безопасности, в результате которого данные становятся доступны неполномочным логическим объектам.

2. Несанкционированный или потенциальный просмотр информации.

1. Компьютер хавфсизлигининг бузилиши, унинг натижасида маълумотлар ваколатга эга бўлмаган мантикий объектларга очик бўлиб қолади.

2. Ахборотни яширин ёки рухсат этилмаган тарзда кўриб чиқиш.

### Распределение ключей

**uz** - калитларни таксимлаш

**en** - key distribution, key management

1. Один из основных механизмов управления ключами. Может реализовываться различными способами. Для симметричных криптосистем возможны варианты доставки ключей абонентам:

– по защищенным каналам, например, при помощи фельдъегерской службы;

– частями по разным каналам;

– через центр распределения ключей.

Для асимметричных криптосистем можно использовать механизм открытого распределения ключей.

2. Совокупность правил, определяющих

## Р

порядок генерации криптографических ключей, рассылки пользователям, хранения и аннулирования.

1. Калитларни бошқаришнинг асосий механизмларидан бири. Турли хил усуллар билан амалга оширилиши мумкин. Симметрик криптотизимлар учун абонентларга калитларни етказиб беришнинг куйидаги вариантлари мавжуд:

- муҳофазаланган каналлар бўйлаб, масалан, фельдъегерлик хизмати ёрдамида;
- турли каналлар бўйлаб қисмларга бўлиб;
- калитларни тақсимлаш маркази орқали.

Асимметрик криптотизимлар учун калитларни очиқ тақсимлаш механизмидан фойдаланиш мумкин.

2. Криптографик калитларни генерациялаш, фойдаланувчиларга юбориш, сақлаш ва бекор қилиш тартибини белгиловчи қоидалар тўплами.

### Распределение ключей открытое

uz - калитларни очиқ тақсимлаш  
en - public key distribution

1. Механизм распределения криптографических ключей по незащищенным каналам телекоммуникаций.

2. Протокол, позволяющий двум абонентам выработать общий секретный ключ путем обмена сообщениями по открытому каналу телекоммуникаций без передачи какой-либо общей секретной информации, распределяемой заранее.

1. Муҳофазаланмаган телекоммуникациялар каналлари бўйича криптографик калитларни тақсимлаш механизми.

2. Иккита абонентга, олдиндан тақсимланмаган қандайдир умумий махфий ахборотни узатмасдан туриб, очиқ телекоммуникациялар канали орқали хабарларни алмашишни йўли билан, умумий махфий калит ишлаб чиқиш

## Р

имконини берадиган протокол.

**Рассеивание**  
**uz** - тарқалиш  
**en** - diffusion

Процесс шифрования, при котором изменение любого знака открытого текста или ключа влияет на большое число знаков шифротекста, что скрывает статистические свойства открытого текста.

Шифрлаш жараёни, бунда очик матннинг хар қандай белгисини ёки калитни ўзгартириш шифрматн белгиларининг кўплаб сонига таъсир кўрсатади, бу эса очик матннинг статистик хусусиятларини беркитади.

**Рассекречивание сведений и их носителей**  
**uz** - маълумотларни ва уларни ташувчиларни ошкор қилиш  
**en** - declassification of information and its carriers

Снятие ранее введенных в предусмотренном законодательством порядке ограничений на распространение сведений, составляющих государственные секреты, и на доступ к их носителям.

Қонунчиликда кўзда тутилган тартибда олдин киритилган, давлат сири ҳисобланадиган маълумотларни тарқатишга ва уларни ташувчилардан фойдалана олишга бўлган чекловларни олиб ташлаш.

**Рассылка спама**  
**uz** - спамни жўнатиш  
**en** - spamming

Рассылка незапрашиваемых данных, которые перегружают систему.

Тизимни ўта банд қиладиган, сўралмаган маълумотларни юбориш.

**Расшифрование**  
**uz** - расшифровка-лаш  
**en** - deciphering

1. Процесс противоположный шифрованию и связанный с восстановлением исходного текста из зашифрованного с использованием известного ключа.

2. Процесс обратного преобразования шифротекста в открытый текст.

1. Шифрлашга карама-қарши ва дастлабки матнни маълум калитдан фойдаланиб, шифр-

## Р

ланган матндан тиклаш билан боғлиқ жараён.  
2. Шифр матнни очик матнга тескари қайта ўзгартириш жараёни.

### Раунд

uz - раунд

en - round

Один шаг шифрования в шифре Файстеля и близких ему по архитектуре шифрах, в ходе которого одна или несколько частей шифруемого блока данных подвергается модификации.

Файстел шифридаги ва архитектура жиҳатдан унга яқин бўлган шифрлардаги шифрлашнинг битга қадами. Шифрлаш жараёнида шифрланадиган блокнинг бир ёки бир нечта қисми ўзгаришга учрайди.

### Регистрация

uz - қайд қилиш

en - log-on

Процедура входа пользователя в систему с указанием идентификационного кода или пароля для получения доступа в систему (сеть).

Фойдаланувчининг, тизимдан (тармокдан) эркин фойдаланиш учун идентификацион код ёки паролни кўрсатган ҳолда, кириш процедураси.

### Регистрация деятельности

uz - фаолиятни

қайд қилиш

uz - activity

registration

Отслеживание действий субъекта доступа или злоумышленника в системе.

Тизимда эркин фойдаланиш субъектининг ёки жинояткорнинг ҳаракатларини кузатиш.

### Регистрация открытого ключа

uz - очик қалитни

рўйхатга олиш

en - public key

registry

Процесс фиксации открытых ключей, обеспечивающий достоверную информацию лицу, осуществляющему запрос, с целью предотвратить фальсификацию значения открытого ключа.

Очик қалитнинг қиймати қалбакилаштирилишини бартараф қилиш мақсадида сў-

## Р

ровни амалга оширувчи шахсга ишончли ахборотни таъминловчи очик калитларни рўйхатга олиш жараёни.

### **Регистрация пользователя**

**uz** - фойдаланувчини рўйхатга олиш  
**en** - user registration

Учет входа пользователя в систему с указанием кода идентификации или пароля для получения доступа в систему.

Фойдаланувчининг тизимга киришини, тизимдан эркин фойдаланиш учун идентификация коди ёки паролни кўрсатган холда, хисобга олиш.

### **Регистр постоянный запоминающий**

**uz** - доимий хотирловчи регистр  
**en** - permanent memory register

Техническое устройство, содержащее данные, которые могут быть прочитаны, но не могут быть изменены.

Ўқиш мумкин бўлган, лекин ўзгартириш мумкин бўлмаган маълумотларни ўз ичига олувчи техник қурилма.

### **Регламентация**

**uz** - қатъий белгилаш  
**en** - regulation

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

Ахборотни муҳофаза қилиш методи. Муҳофаза қилинаётган ахборотни автоматлаштирилган қайта ишлаш, уни сақлаш ва узатишининг шундай шароитлари яратиладики, натижада ахборотдан рухсат этилмаган тарзда фойдалана олиш имкониятлари минимумга келтирилади.

### **Режим использования защищенный**

**uz** - муҳофазаланган фойдаланиш

Режим защищенной обработки базы данных, в котором все прикладные программы, работающие параллельно с программой, открывшей области базы данных в этом режиме, могут читать записи, но не могут

## Р

- режими  
**en** - protected usage mode
- их обновлять до тех пор, пока программа не закрывает эти области
- Режим обхода**  
**uz** - четлаб ўтиш режими  
**en** - by-pass mode
- Режим работы оборудования шифрования данных, при котором открытый текст передается без искажения.
- Режим разграничения доступа**  
**uz** - эркин фойдаланишни чегаралаш режими  
**en** - access demarcation mode
- Маълумотларни шифрлаш ускунасининг ишлаш режими бўлиб, бунда очик матн бузилмасдан узатилади.
- Порядок доступа лиц к техническим средствам, программе при ее обработке на средствах вычислительной техники в соответствии с заранее разработанными и утвержденными правилами.
- Резидентный**  
**uz** - резидент  
**en** - resident
- Шахсларнинг, олдиндан ишлаб чиқилган ва тасдиқланган қоидаларга мувофиқ, ҳисоблаш техникаси воситаларидан, қайта ишлашда дастурдан фойдалана олиш тартиби.
- Постоянно присутствующий в оперативной памяти.
- Реконструкция данных**  
**uz** - маълумотларни тиклаш  
**en** - data reconstruction
- Оператив хотирада доимо мавжуд бўладиган.
- Метод реставрации данных путем анализа первоисточников.
- Асл манбани таҳлил қилиш йўли билан маълумотларни реставрация қилиш методи.

## Р

### **Реставрация данных**

**uz** - маълумотларни реставрация қилиш  
**en** - data restoration

Восстановление потерянных или зараженных данных.

*Примечание: Совокупность метода копирования архивных данных, метода реконструкции данных из исходных данных или метода восстановления данных из альтернативных источников.*

Йўқолган ёки зарарланган маълумотларни тиклаш.

*Изоҳ: Архив маълумотларидан нусха кўчириш, маълумотларни дастлабки маълумотлардан тиклаш ёки маълумотларни муқобил манбалардан ҳосил қилиш методларининг жами.*

### **Ресурс**

**uz** - ресурс  
**en** - resource

Любой из компонентов вычислительной системы и предоставляемые ею возможности.

Ҳисоблаш тизими компонентларидан исталгани ҳамда бу тизим томонидан тақдим этиладиган имкониятлар.

### **Ресурс защищенный**

**uz** - муҳофазаланган ресурс  
**en** - locked resource

Ресурс, для которого определен замок защиты (секретности), т.е. управление доступом специфицировано

Муҳофаза (махфийлик) кулфи белгиланган, яъни эркин фойдаланишни бошқариш спецификацияланган (таснифланган) ресурс.

### **Ресурсы информационные**

**uz** - ахборот ресурслари  
**en** - information resources

Отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах)

Алоҳида ҳужжатлар ва ҳужжатларнинг алоҳида массивлари, ахборот тизимларидаги (кутубхона, архив, фонд, маълумотлар банки, бошқа ахборот тизимлари) ҳужжатлар ва ҳужжатларнинг массивлари.

### **Решение по защи-**

Техническое, планировочное, архитектур-



## Р

**те информации  
техническое**

**uz** - ахборотни

муҳофаза қилиш  
бўйича техник ечим

**en** - technical solu-  
tion on information  
security

ное или конструкторское решение по защите информации.

Ахборотни муҳофаза қилиш бўйича техник, лойиҳа, архитектура ёки конструкторлик ечими.

**Решетка Кардано**

**uz** - Кардано пан-  
жараси

**en** - Cardano grid

Криптографическая система, реализующая шифр перестановок. Представляет собой квадратную таблицу (решетку), в которой четверть ячеек прорезана так, чтобы при четырех поворотах покрывать всю таблицу. Открытый текст вписывается в прорезанные ячейки решетки, которая поворачивается на  $90^0$ , открывая тем самым новые, незаполненные ячейки.

Алмаштириб қўйиш шифрини амалга оширувчи криптографик тизим. Ўзида ячейкаларнинг тўртдан бири тўрт бурилишда барча жадвални қамраб оладиган тарзда кесилган квадрат жадвал (панжара)ни акс эттиради. Очк матн  $90^0$  га буриладиган панжаранинг кесилган ячейкаларига ёзилади, шу билан янги, тўлдирилмаган ячейкалар очилади.

**Решетка кодовая**

**uz** - кодли панжара

**en** - code grid

Направленный граф, в который превращается дерево сверхточного кода с конечной длиной ограничения.

Йўналтирилган граф бўлиб, унга охирги чеклаш узунлигига эга юқори аниқликдаги код дарахти айланади.

**Риск**

**uz** - риск

(эҳтимолий хавф)

**en** - risk

Возможность использования конкретной уязвимости системы обработки данных при реализации конкретной угрозы.

## Р

Муайян хавфни амалга оширишда маълумотларни қайта ишлаш тизимининг муайян заифлигидан фойдаланиш имконияти.

### Ряд

**uz** - қатор

**en** - family

Семейство ЭВМ, использующих единое программное обеспечение.

Ягона дастурий таъминотдан фойдаланувчи ЭХМ туркуми.

## С

### Самокодирование

**uz** - ўзини ўзи кодлаш

**en** - intrinsic coding

Кодирование информации с использованием самой информации в качестве ключа.

Ахборотни, калит сифатида ахборотнинг ўзидан фойдаланиб, кодлаш.

### Сборка «мусора»

**uz** - «ахлат» йиғиш

**en** - garbage collection

Атака, заключающаяся в поиске информации, остающейся в оперативной памяти или на накопителях информации после работы субъекта либо объекта системы.

Субъект ёки тизим объекти ишидан сўнг, оператив хотира ёки ахборот тўплагичларда қолган ахборотни излашдан иборат хужум.

### Сведения особой важности

**uz** - алоҳида муҳим маълумотлар

**en** - highly important information

Наиболее охраняемые государством сведения из числа составляющих государственные секреты.

Давлат томонидан қаттиқ муҳофаза қилинадиган, давлат сири ҳисобланадиган маълумотлар таркибига қирадиган маълумотлар.

### Сведения секретные

**uz** - махфий маълумотлар

**en** - secret informations

Сведения, составляющие служебную тайну.

Хизмат сири ҳисобланадиган маълумотлар.

## С

### **Сведения совершенно секретные**

**uz** - мутлако махфий маълумотлар  
**en** - top secret informations

### **Секретность информации**

**uz** - ахборотнинг махфийлиги  
**en** - information secrecy

### **Секретность совершенная**

**uz** - мукаммал махфийлик  
**en** - unconditional secrecy

### **Секреты государственные**

**uz** - давлат сирлари  
**en** - state secrets

Сведения, составляющие государственную тайну за исключением сведений особой важности.

Алохида мухим маълумотлардан ташкари давлат сири ҳисобланадиган маълумотлар.

Свойство информации, обеспечивающее при ее обработке техническими средствами предотвращение несанкционированного ознакомления с ней или несанкционированного документирования (снятия копий).

Ахборотнинг уни техник воситалар билан қайта ишлашда ахборотдан рухсат этилмаган тарзда танишишнинг ёки ҳужжатлаштиришнинг (нусхалар олишнинг) барта-раф этилишини таъминловчи хоссаси.

Условие, заключающееся в том, что открытый текст и шифротекст статистически независимы и получение (перехват) шифротекста не дает криптоаналитику дополнительной информации об открытом тексте.

Очиқ матн ва шифр матн статистик жиҳатдан мустақил ва шифрматнни олиш (қўлга киритиш) криптоаналитикка очик матн тўғрисида қўшимча ахборот бермайдиган шароит.

Защищенные государством сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Республики Узбекистан. Государственные секреты делятся по степени секретности на сведения особой важности и совер-

## С

шенно секретные (государственная тайна).

Тарқатилиши Ўзбекистон Республикаси манфаатларига зиён келтириши мумкин бўлган ҳарбий, ташқи сиёсий, иқтисодий, илмий-техникавий, разведка, контрразведка билан шуғулланувчи ва оператив-қидирув фаолияти соҳасидаги давлат томонидан муҳофаза қилинадиган маълумотлар. Давлат сирлари махфийлик даражасига кўра, алоҳида муҳим маълумотлар ва мутлақо махфий (давлат сири) маълумотларга бўлинади.

### **Сектор дополнительный**

**uz** - қўшимча сектор

**en** - extra sector

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

Нусха кўчиришдан муҳофаза қилиш методининг қисми, бунда йўлгага секторларнинг стандарт микдоридан ортиқ яна битта сектор ёзилади.

### **Сектор ложный**

**uz** - чалғитувчи сектор

**en** - false sector

Сектор, состоящий только из одного заголовка без данных, многократно записываемый на диск, чтобы его было невозможно скопировать с помощью программы не-санкционированного копирования.

Маълумотларсиз, фақат сарлавҳадан иборат бўлган, уни рухсат этилмаган тарзда нусха кўчириш дастури ёрдамида кўпайтириш мумкин бўлмаслиги учун дискка кўп марта ёзиб олиннадиган сектор.

### **Сервер-посредник**

**uz** - воситачи сервер

**en** - proxy server

Межсетевой экран, в котором для преобразования IP-адресов всех авторизованных клиентов в IP-адреса, ассоциированные с межсетевым экраном, используется процесс, называемый трансляцией адресов.

## С

Тармоқлараро экран, унда барча муаллиф-лаштирилган мижозларнинг IP адресларини тармоқлараро экран билан ассоциацияланган IP адресларга ўзгартириш учун адресларни трансляция қилиш деб аталадиган жараёндан фойдаланилади.

### **Сертификат**

**uz** - сертификат

**en** - certificate

Набор относящихся к обеспечению безопасности данных, который выдан органом обеспечения безопасности или пользующейся доверием третьей стороной, в совокупности с информацией о безопасности, используемой для предоставления услуг обеспечения целостности и аутентификации источника данных в отношении данных.

Хавфсизликни таъминлаш органи ёки ишонч қозонган учинчи томон берган, хавфсизликни таъминлашга тааллуқли бўлган, маълумотлар манбаини аутентификация қилишни таъминлаш хизматларини тақдим этиш учун фойдаланиладиган, хавфсизлик тўғрисидаги ахборот билан биргаликдаги маълумотлар тўплами.

### **Сертификат авторизации**

**uz** - муаллифлаштириш сертификати

**en** - authorization certificate

Электронный документ, подтверждающий право доступа к информации, личность пользователя или иные его права и полномочия.

Ахборотдан эркин фойдаланиш ҳуқуқини, фойдаланувчининг шахсини ёки унинг бошқа ҳуқуқлари ва ваколатларини тасдиқловчи электрон ҳужжат.

### **Сертификат аннулирования**

**uz** - бекор қилиш сертификати

**en** - revocation

Сертификат безопасности, выданный органом безопасности для указания, что конкретный сертификат безопасности был аннулирован.

## С

certificate

Хавфсизлик органи томонидан муайян хавфсизлик сертификати бекор қилинганлигини кўрсатиш учун бериладиган хавфсизлик сертификати.

**Сертификат атрибута**

**uz** - атрибут сертификати

**en** - attribute certificate

Структура данных, имеющая цифровую подпись органа по присвоению атрибутов, которая связывает некоторые значения атрибутов с идентификационной информацией о держателе этого атрибута.

Атрибутларни бериш органининг рақамли имзосига эга бўлган, атрибуларнинг баъзи қийматларини бу атрибуларнинг эгаси тўғрисидаги идентификацион ахборот билан боғлайдиган маълумотлар структураси.

**Сертификат аутентификации**

**uz** - аутентификация қилиш сертификати

**en** - authentication certificate

Сертификат безопасности, который гарантирован органом сертификации и может быть использован для обеспечения идентификации объекта.

Сертификатлаш органи томонидан қўллашган ва объектнинг идентификация қилинишини таъминлаш учун фойдаланилиши мумкин бўлган хавфсизлик сертификати.

**Сертификат безопасности**

**uz** - хавфсизлик сертификати

**en** - security certificate

Набор связанных с безопасностью данных, выданных органом безопасности или пользующейся доверием третьей стороной, вместе с информацией безопасности, которая используется для обеспечения услуг целостности и аутентификации источника данных.

Хавфсизлик органи ёки ишонч қозонган учинчи томон берган хавфсизлик билан боғлиқ маълумотларнинг маълумотлар манбаини аутентификация қилиш ва маълумотларнинг яхлитлигини таъминлаш учун

фойдаланиладиган хавфсизлик ахбороти билан биргаликдаги тўплами.

**Сертификат за-  
щиты**

**uz** - муҳофаза қилиш сертификати  
**en** - protection certificate

1. Документ, удостоверяющий соответствие средств вычислительной техники или автоматизированной системы набору требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и/или распространение их как защищенных.

2. Надлежащим образом оформленный документ, выданный по правилам системы сертификации и подтверждающий соответствие средства защиты информации требованиям по безопасности информации.

1. Ҳисоблаш техникаси ёки автоматлаштирилган тизим воситаларининг ахборотдан рухсат этилмаган тарзда фойдалана олишдан муҳофаза қилиш бўйича талабларга мувофиқлигини тасдиқловчи ва ишлаб чиқувчи ахборотдан муҳофазаланган ахборот сифатида фойдаланиш ва ёки тарқатиш ҳуқуқини берадиган ҳужжат.

2. Тегишли равишда расмийлаштирилган, сертификатлаш тизими қодаларига кўра берилган ва ахборотни муҳофаза қилиш воситаларининг ахборот хавфсизлиги бўйича талабларга мувофиқ келишини тасдиқловчи ҳужжат.

**Сертификат ключа**

**uz** - калит сертификати  
**en** - key certificate

Цифровое свидетельство, подтверждающее соответствие открытого ключа лицу, его выработавшему. В самой простой форме сертификаты содержат открытый ключ и имя автора ключа. Кроме этой информации, в сертификате также может содержаться дата окончания срока действия сертификата, название организации, выдавшей сертификат, и некоторая другая информация.

## С

Очиқ калитнинг уни ишлаб чикувчи шахсга мувофиқлигини тасдиқловчи рақамли гувоҳнома. Энг оддий шаклда сертификатлар очиқ калитни ва калит муаллифининг номини ўз ичига олади. Бу ахборотдан ташқари, сертификатда сертификатнинг амал қилиш муддати тугаган сана, сертификат берган ташкилот номи ва айрим бошқа ахборот бўлиши мумкин.

### **Сертификат органи**

**uz** - орган сертификати

**en** - authority certificate

Сертификат, выданный органу (например, органу сертификации или органу по присвоению атрибутов).

Органга (масалан, сертификатлаш органига ёки атрибутларни бериш бўйича органга) берилган сертификат.

### **Сертификат открытого ключа**

**uz** - очиқ калит сертификати

**en** - public key certificate

1. Открытый ключ пользователя и некоторая другая информация, не поддающаяся подделке благодаря шифрованию, вместе с личным ключом выдавшего его органа сертификации.

2. Значения, представляющие собой открытый ключ владельцев (и другую факультативную информацию), которые проверены и подписаны доверенным органом в формате, не поддающемся подделке.

1. Фойдаланувчининг очиқ калити, уни берган сертификатлаш органининг шахсий калити билан бирга, шунингдек, шифрлаш туфайли қалбакилаштириб бўлмайдиган баъзи бир бошқа ахборот.

2. Қалбакилаштириб бўлмайдиган форматда ваколатли орган томонидан текширилган ва имзоланган, ўзида эгаларининг очиқ калитини (бошқа ихтиёрый ахборотни) ифодалайдиган қўйматлар.



## С

### **Сертификат соответствия**

**uz** - мувофиқлик сертификати  
**en** - conformance certificate

Документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы требованиям государственных стандартов, иных нормативных документов по защите информации, утвержденных государственными органами по сертификации в пределах их компетенции, и дающий право разработчику на эксплуатацию и/или распространение их как защищенных.

Хисоблаш техникаси воситалари ёки автоматлаштирилган тизимнинг, давлат стандартлари талабларига, сертификатлаш бўйича давлат органлари томонидан, уларнинг ваколатлари доирасида тасдиқланган ахборотни муҳофаза қилиш бўйича бошқа норматив ҳужжатлар талабларига мувофиқлигини тасдиқловчи ва ишлаб чиқувчига улардан муҳофаза қилинган ҳужжат сифатида фойдаланиш ва ёки тарқатиш ҳуқуқини берувчи ҳужжат.

### **Сертификат списка аннулирования**

**uz** - бекор қилиш рўйхатининг сертификати  
**en** - revocation list certificate

Сертификат безопасности, определяющий список сертификатов безопасности, которые были аннулированы.

Бекор қилинган хавфсизлик сертификатларининг рўйхатини белгиловчи хавфсизлик сертификати.

### **Сертификат цифровой**

**uz** - рақамли сертификат  
**en** - digital certificate

1. Электронный документ, которым доверенное третье лицо снабжает открытый ключ пользователя. Сертификат подтверждает, что срок действия ключа не истек и он действительно принадлежит пользователю.

2. Набор данных, который объединяет название организации или имя физического лица и его открытый ключ.

## С

1. Ишончли учинчи шахс фойдаланувчининг очик калитини таъминлайдиган электрон хужжат. Сертификат калитнинг амал қилиш муддати тугамаганлигини ва у ҳақиқатдан фойдаланувчига тегишли эканлигини тасдиқлайди.
2. Ташкилот номини ёки жисмоний шахс исмини ҳамда унинг очик калитини бирлаштирадиган маълумотлар тўплами.

**Сертификация**  
**uz** - сертификатлаш  
**en** - certification

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

Маълумотларни қайта ишлаш тизими ёки унинг қисми хавфсизлик талабларига мос келишини учинчи томон кафолатлайдиган процедура.

**Сертификация**  
**системы защиты**  
**информации**  
**uz** - ахборотни муҳофаза қилиш тизимини сертификатлаш  
**en** - information security system certification

Деятельность по подтверждению соответствия системы защиты информации требованиям государственных стандартов, иных нормативных документов по защите информации, утвержденных государственными органами по сертификации в пределах их компетенции.

Ахборотни муҳофаза қилиш тизимининг давлат стандартлари талабларига, сертификатлаш бўйича давлат органлари томонидан уларнинг ваколатлари доирасида тасдиқланган ахборотни муҳофаза қилиш бўйича бошқа норматив хужжатларнинг талабларига мувофиқлигини тасдиқлаш бўйича фаолият.

**Сертификация**  
**соответствия в**  
**области защиты**

Деятельность по подтверждению соответствия средств защиты информации требованиям государственных стандартов или

## С

### **информации**

**uz** - ахборотни муҳофаза килиш соҳасида мувофиқликни сертификатлаш  
**en** - conformance certificate in the information security field

### **Сеть телекоммуникаций**

**общего пользования защищенная уз** – муҳофазаланган умумий фойдаланишдаги телекоммуникациялар тармоғи  
**en** - protected public switched telecommunications network

инных нормативных документов по защите информации.

Ахборотни муҳофаза килиш воситаларининг ахборотни муҳофаза килиш бўйича давлат стандартлари ёки бошқа норматив ҳужжатларнинг талабларига мувофиқлигини тасдиқлаш бўйича фаолият.

Сеть телекоммуникаций общего пользования, в которой любое воздействие нарушителя (из множества заданных при проектировании) либо не допускается с заданной вероятностью, либо обнаруживается средствами сети с заданной вероятностью, иницируя при этом реакцию сети, направленную на ликвидацию с заданной вероятностью последствий этого воздействия: информирование пользователей, локализацию места воздействия, восстановление работоспособности сети и создание условий, обеспечивающих передачу информации (данных) пользователей.

Умумий фойдаланишдаги телекоммуникациялар тармоғи, бунда бузғунчининг ҳар қандай таъсирига (лойихалашда берилган кўпикдан), ё берилган эҳтимоллик билан йўл қўйилмайди, ё тармоқ воситалари билан берилган эҳтимолликда аниқланади, бунда тармоқнинг ушбу таъсирнинг оқибатларини берилган эҳтимолликда бартараф қилишга йўналтирилган жавоби: фойдаланувчиларни хабардор қилиш, таъсир жойининг кенгайишига йўл қўймаслигини, тармоқнинг иш қобилиятини тиклаш ва фойдаланувчиларнинг ахбороти (маълумотлари) узатилишини таъминловчи шароитлар яратилади.

## С

**Сеть Файстеля**  
**uz** - Файстель  
тармоғи  
**en** - Feistel network

Архитектура построения блочных шифров, доминирующая в настоящее время в традиционной криптографии, в которой весь процесс шифрования блока выполняется за серию шагов (раундов), на каждом из которых блок делится на изменяемую и постоянную части. С помощью функции шифрования из постоянной части и раундового ключа вырабатывается модифицирующий код, который используется для модификации изменяемой части посредством операции гаммирования.

Блокли шифрлар тузиш архитектураси. Бунда блокни шифрлашнинг бутун жараёни кадамлар (раундлар) ичида бажарилади. Уларнинг ҳар бирида блок ўзгарадиган ва ўзгармайдиган қисмларга ажратилади. Шифрлаш функцияси ёрдамида ўзгармайдиган қисм ва раунд калитидан гаммалаш операцияси воқитасида ўзгарадиган қисмни модификациялашда фойдаланиладиган модификацияловчи код ишлаб чиқилади.

**Сигнал информативный**  
**uz** - информатив  
сигнал  
**en** - informative  
signal

Физический сигнал или химическая среда, содержащие информацию с ограниченным доступом.

**Сигнатура**  
**uz** - сигнатура  
**en** - signature

Фойдаланилиши чекланган ахборотни ўз ичига олувчи физик сигнал ёки кимёвий муҳит.

1. Уникальная характеристика системы, которая может быть проверена программным способом. Примером сигнатуры может служить вторичный признак диска, используемый в качестве идентификационной метки диска-оригинала. Этот признак не должен копироваться программным способом.

2. Участок постоянного кода программы, по

## С

которому антивирусные программы обычно определяют принадлежность программ к программам-вирусам и другим нежелательным типам программ.

1. Тизимнинг дастурий усулда текшириш мумкин бўлган ноёб характеристикаси. Оригинал-дискнинг идентификацион белгиси сифатида қўлланиладиган дискнинг иккинчи белгиси сигнатурага мисол бўлади. Бу белгидан дастурий усулда нусха кўчириш мумкин эмас.

2. Дастур доимий кодининг қисми, унга қараб, вирусга қарши дастурлар дастурларнинг вирус дастурларга ва дастурларнинг бошқа номақбул турларига мансублигини аниқлайди.

**Сигнатура вируса**  
**uz** - вирус сигнату-  
раси  
**en** - virus signature

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

Битларнинг специфик вируснинг ҳар бир нусхасига хос бўлган ва унинг мавжудлигини аниқлаш учун сканловчи дастур томонидан фойдаланилиши мумкин бўлган ягона кетма-кетлиги.

**Символ управ-  
ляющий**  
**uz** - бошқарувчи  
символ  
**en** - control character

Байт кода ASCII, который не выводится на печать, но управляет компьютером, принтером или другим устройством.

ASCII кодининг байти, у компьютердан чиқарилмайди, лекин компьютер, принтер ёки бошқа қурилмани бошқаради.

**Система автома-  
тизированная в**

Автоматизированная система, реализующая информационную технологию выполнения

## С

**защищённом исполнении**

**uz** - муҳофаза қилинган автоматлаштирилган тизим  
**en** - automatized system in guarded construction

**Система анализа защищенности**

**uz** - муҳофаза қилинганликни таҳлил қилиш тизими  
**en** - protection analysis system

**Система восстановления**

**uz** - тиклаш тизими  
**en** - recovery system

**Система замков и ключей**

**uz** - қулфлар ва қалитлар тизими  
**en** - locks and keys (system)

установленных функций в соответствии с требованиями стандартов и/или нормативных документов по защите информации.

Ахборотни муҳофаза қилиш бўйича стандартлар ва ёки норматив ҳужжатларнинг талабларига мувофиқ белгиланган функциялар бажарилишининг ахборот технологиясини амалга оширадиган автоматлаштирилган тизим.

Техническое или программное средство, предназначенное или используемое для анализа защищенности технических средств или автоматизированной системы.

Техник воситалар ёки автоматлаштирилган тизимнинг муҳофаза қилинганлигини таҳлил қилиш учун мўлжалланган ёки ишлатиладиган техник ёки дастурий восита.

Комплекс программ и управляющих таблиц, предназначенных для поддержания целостности данных. Используется в банках данных и других автоматизированных системах.

Маълумотларнинг яхлитлигини таъминлашга қаратилган дастурлар ҳамда бошқарувчи жадваллар комплекси. Маълумотлар банкида ва бошқа автоматлаштирилган тизимларда фойдаланилади.

Система защиты памяти, в которой сегментам памяти операционной системой присвоены идентификационные номера – замки, а зарегистрированным пользователям, числовые коды – ключи.

Хотирани муҳофаза қилиш тизими. Унда

хотира сегментларига операциялар тизим томонидан идентификацион рақамлар – кулфлар, рўйхатга олинган фойдаланувчиларга эса сонли кодлар – калитлар берилди.

**Система защиты информации**

**uz** - ахборотни муҳофаза қилиш тизими

**en** - information security system

Совокупность органов и/или исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.

Ахборотни муҳофаза қилиш соҳасига тегишли ҳуқуқий, ташкилий-фармойиш берувчи ва норматив ҳужжатлар билан белгиланган қоидалар бўйича ташкил қилинган ҳамда фаолият кўрсатадиган органлар ва/ёки ижро этувчилар, улар томонидан фойдаланиладиган ахборотни муҳофаза қилиш техникасининг жами.

**Система защиты информации (данных)**

**uz** - ахборот (маълумотлар)ни муҳофаза қилиш тизими

**en** - information (data) protection system

1. Комплекс аппаратных, программных и криптографических средств, а также мероприятий, обеспечивающих защиту информации (данных) от случайного или преднамеренного разрушения, искажения или использования.

2. Совокупность (комплекс) специальных мер правового (законодательного) и административного характера, организационных мероприятий, физических и технических (программных и аппаратных) средств защиты, а также специального персонала, предназначенных для обеспечения безопасности автоматизированной системы или циркулирующей в ней информации.

1. Аппарат, дастурий ва криптографик во-

## С

ситалар, шунингдек, ахборот (маълумотлар)нинг тасодифий ёки қасддан бузишдан, бузиб кўрсатилишдан ёки фойдаланишдан муҳофаза қилинишини таъ-минловчи тадбирлар комплекси.

2. Хуқуқий (қонуний) ва маъмурий характердаги махсус чора-тадбирлар, ташкилий тадбирлар, жисмоний ва техник (дастурий ва аппарат) муҳофаза воситалари, шунингдек, автоматлаштирилган тизим ёки унда айланадиган ахборотнинг хавфсизлигини таъминлаш учун мўлжалланган махсус персоналнинг жами (комплекси).

**Система защиты информации от несанкционированного доступа**

**uz** - ахборотни рухсатсиз фойдалана олишдан муҳофаза қилиш тизими  
**en** - unauthorized access data protection system

Комплекс организационных мер и программно-технических (в том числе и криптографических) средств защиты информации от несанкционированного доступа к информации в автоматизированных системах.

Автоматлаштирилган тизимларда ахборотни рухсат этилмаган тарзда фойдалана олишдан муҳофаза қилиш бўйича кўриладиган ташкилий чора-тадбирлар ва дастурий-техник (шу жумладан, криптографик) воситалар комплекси.

**Система защиты одноступенчатая**

**uz** - бир поғонали муҳофаза тизими  
**en** - key to the door protection

Система защиты, в которой единственный ключ обеспечивает доступ к программному обеспечению.

Ягона калит дастурий таъминотдан фойдаланишни таъминлайдиган муҳофаза қилиш тизими.

**Система защищенная**

**uz** - муҳофаза қилинган тизим  
**en** - protected system

Система, вход в которую требует ввода пароля.

Кириш учун паролнинг киритилиши талаб этиладиган тизим.



## С

### **Система идентификации**

**uz** - идентификациялаш тизими  
**en** - identification system,  
ID system

Криптографическая система, выполняющая функцию аутентификации сторон в процессе информационного взаимодействия.

Ахборотга оид (информацион) ўзаро ҳамкорлик жараёнида томонларни аутентификация қилиш функциясини бажарадиган криптографик тизим.

### **Система избыточная**

**uz** - ортикча тизим  
**en** - redundant system

Система, обладающая избыточностью некоторого типа аппаратной, алгоритмической, информационной, обеспечивающей повышение надежности ее функционирования.

Тизимнинг ишончли ишлаш даражаси ошишини таъминловчи, қандайдир турдаги аппарат, алгоритм, ахборот ортикчалигига эга тизим.

### **Система имитозащиты**

**uz** - имитомуҳофаза тизими  
**en** - protection system from falsified data

Криптографическая система, выполняющая функцию аутентификации содержания сообщения либо документа и предназначенная для защиты от несанкционированной модификации информации или навязывания ложной информации.

Хабар ёки хужжат мазмунини аутентификация қилиш функциясини бажарадиган ва ахборотни рухсат этилмаган тарзда ўзгаририлишдан ёки сохта ахборотнинг мажбуран киритилишидан (қабул қилинишидан) муҳофаза қилиш учун мўлжалланган криптографик тизим.

### **Система информационная**

**uz** - ахборот тизими  
**en** - information system

Организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и телекоммуникаций, реализующих информационные процессы.

## С

Хужжатлар (хужжатлар массиви) ва ахборот технологияларининг, шу жумладан, ахборот жараёнларини амалга оширувчи ҳисоблаш техникаси ва телекоммуникациялар воситаларидан фойдаланиб, ташкилий равишда тартибга солинган тўплами.

**Система информационная автоматизированная**  
**uz** - автоматлаштирилган ахборот тизими

**en** - automated information system,  
**AIS**

Совокупность программных и аппаратных средств, предназначенных для создания, передачи, обработки, распространения, хранения и/или управления данными и информацией и производства вычислений.

Ахборот ва маълумотларни яратиш, узатиш, қайта ишлаш, тарқатиш, сақлаш ва ёки бошқариш, шунингдек, ҳисоблашларни амалга ошириш учун мўлжалланган дастурий ва аппарат воситаларнинг жами.

**Система информационная защищенная**  
**uz** – муҳофазаланган ахборот тизими  
**en** - protected information system

Информационная система, в которой реализованы механизмы выполнения правил, удовлетворяющих установленному на основе анализа угроз перечню требований по защите информации и компонентов этой системы.

Таҳдидларни таҳлил қилиш асосида ўрнатилган, ахборотни ҳамда тизим компонентларини муҳофаза қилиш бўйича талаблар рўйхатини қондирадиган қоидаларнинг бажарилиш механизми амалга оширилган ахборот тизими.

**Система ключевая**  
**uz** - калит тизими  
**en** - key system

1. Совокупность правил, определяющих порядок генерации, распределения, использования, хранения, смены, уничтожения и восстановления криптографических ключей.
2. Совокупность криптографических ключей и правил обращения с ними при обес-

## С

печении криптографической защиты информации.

1. Криптографик калитларни генерация қилиш, таксимлаш, улардан фойдаланиш, сақлаш, алмаштириш, йўқ қилиш ва тиклаш тартибини белгиловчи қоидалар тўплами.

2. Ахборотнинг криптографик муҳофаза қили-нишини таъминлашда, криптографик калитлар ва улардан фойдаланиш қоидаларининг тўплами.

**Система кодирования**

**uz** - кодлаш тизими  
**en** - coding system

Совокупность символов и правил кодирования; код.

Кодлаш символлари ва қоидаларининг йиғиндиси; код.

**Система компьютерная достоверная**

**uz** - ишончли компьютер тизими  
**en** - trusted computer system

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

2. Система, обеспечивающая ведение безопасной обработки несортированного потока критичной информации за счет использования аппаратных и программных средств обеспечения безопасности.

1. Фойдаланувчиларнинг махфийлик грифлари ва хавфсизлик категориялари турлича бўлган маълумотлардан бир вақтда фойдалана олиш имконияти ҳисобга олинган ҳолда, етарлича компьютер хавфсизлиги кўзда тутиладиган маълумотларни қайта ишлаш тизими.

2. Хавфсизликни таъминлашнинг аппарат ва дастурий воситаларидан фойдаланиш ҳисобига сараланмаган критик ахборот

## С

оқимининг қайта ишланиши хавфсиз олиб  
борилишини таъминловчи тизим.

**Система крипто-  
графическая**  
**uz** - криптографик  
тизим  
**en** - cryptographic  
system,  
cryptosystem

1. Семейство выбираемых с помощью ключа обратимых преобразований, которые преобразуют открытый текст в шифротекст и обратно.  
2. Совокупность технических и/или программных средств, организационных методов, обеспечивающих криптографическое преобразование информации и управление процессом распределения ключей.

1. Очiq маттни шифр матнга ва аксинча, ўзгартирадиган қайта ўзгартиришларнинг калит ёрдамида танлаб олинадиган туркуми.  
2. Ахборотнинг криптографик қайта ўзгартирилишини ва калитларни тақсимлаш жараёни бошқарилишини таъминловчи техник ва/ёки дастурий воситалар, ташкилий методларнинг жами.

**Система крипто-  
графической защи-  
ты информации**  
**uz** - ахборотни  
криптографик  
муҳофаза қилиш  
тизими  
**en** - data cryptop-  
rotection system

Система, осуществляющая криптографическое преобразование информации для обеспечения ее безопасности.

Ахборотнинг, унинг хавфсизлигини таъминлаш максатида, криптографик қайта ўзгартирилишини амалга оширувчи тизим.

**Система (служба)  
обеспечения ин-  
формационной  
безопасности,  
(СОИБ)**  
**uz** - ахборот хав-  
фсизлигини  
таъминлаш тизими

Совокупность правовых, организационных и технических мероприятий, средств и норм, направленных на предотвращение или существенное затруднение нанесения ущерба интересам собственника информации.

Ахборот эгаси манфаатларига зиён келти-

## С

(хизмати) (АХТТ)  
**en** - information security supporting system (service)

**Система обеспечения информационной безопасности**

**uz** - ахборот хавфсизлигини таъминлаш тизими  
**en** - information security system

**Система обеспечения информационной безопасности сети телекоммуникаций общего пользования**

**uz** - умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавфсизлигини таъминлаш тизими  
**en** - public switched telecommunications network information security system

**Система обнаружения атак**

рилишини бартараф қилиш ёки жиддий қийинлаштиришга йўналтирилган, ҳуқуқий, ташкилий ва техник тадбирлар, воситалар ва нормалар жами.

Совокупность органов и/или исполнителей, используемые ими средства защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами.

Органлар ёки бажарувчилар жами, улар фойдаланадиган ахборотни муҳофаза қилиш воситалари, шунингдек, тегишли ҳуқуқий, ташкилий-фармойиш берувчи ва норматив ҳужжатлар билан белгиланган қоидалар бўйича ташкил қилинган ва иш юритадиган муҳофаза объектлари.

Совокупность правовых, организационных и технических мероприятий, служб и механизмов информационной безопасности, норм, органов управления и исполнителей в определенной сети телекоммуникаций общего пользования, направленных на обеспечение ее информационной безопасности.

Умумий фойдаланишдаги муайян телекоммуникациялар тармоғидаги, бу тармоқнинг ахборот хавфсизлигини таъминлашга қаратилган ҳуқуқий, ташкилий ва техник тадбирлар, ахборот хавфсизлиги хизматлари ва механизмлари, нормалар, бошқарув органлари ва бажарувчилар жами.

Техническое или программное средство, предназначенное или используемое для

**uz** - хужумларни аниқлаш тизими  
**en** - intrusion detection system

обнаружения атак на ресурсы системы.

**Система обработки информации автоматизированная**

**uz** - автоматлаштирилган ахборотни қайта ишлаш тизими  
**en** - automated data processing system

Тизим ресурсларига қилинадиган хужумни аниқлаш учун мўлжалланган ёки ишлатиладиган техник ёки дастурий восита.

Организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов: технических средств обработки и передачи данных (средств вычислительной техники и связи), методов и алгоритмов обработки в виде соответствующего программного обеспечения, массивов (наборов, баз) данных на различных носителях, персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных с целью удовлетворения информационных потребностей государственных органов, общественных или коммерческих организаций (юридических лиц), отдельных граждан (физических лиц) и иных потребителей информации.

Куйидаги ўзаро боғланган компонентларнинг жамини ўзида ақс эттирувчи ташкилий-техник тизим: маълумотларни қайта ишлаш ва узатиш техник воситалари (ҳисоблаш техникаси ва алоқа воситалари), тегишли дастурий таъминот кўринишидаги қайта ишлаш методлари ва алгоритмлари, турли ташувчилардаги маълумот массивлари (тўшпамлари, базалари), давлат органлари, жамоат ёки тижорат ташкилотлари (юридик шахслар), айрим фуқаролар (жисмоний шахслар) ва ахборот бошқа истеъмолчиларининг ахборотга бўлган эҳтиёжларини қондириш мақсадида, маълумот-

## С

ларни автоматлаштирилган тарзда қайта ишлашни бажариш учун ташкилий-структура, тематик, технологик ёки бошқа белгиларга кўра бирлаштирилган персонал ва фойдаланувчилар.

**Система операционная**

**uz** - операцион тизим

**en** - operating system

Главная часть программного обеспечения, которая координирует и управляет ресурсами ЭВМ.

Дастурий таъминотнинг ЭХМ ресурсларини мувофиқлаштирадиган ва бошқарадиган асосий қисми.

**Система операционная безопасная**  
**uz** - хавфсиз операцион тизим

**en** - secure operating system

Операционная система, эффективно управляющая аппаратными и программными средствами с целью обеспечения уровня защиты, соответствующего содержанию данных и ресурсов, контролируемых этой системой.

Тизим томонидан назорат қилинадиган маълумотлар ва ресурслар мазмунига мос келадиган муҳофаза даражасини таъминлаш мақсадида аппарат ва дастурий воситаларни самарали бошқарадиган операцион тизим.

**Система сертификации в области защиты информации**

**uz** - ахборотни

муҳофаза қилиш соҳасида сертификация катлаш тизими

**en** - certification system in the field of information security

Система, располагающая собственными правилами, процедурами и управлением для проведения сертификации соответствия в области защиты информации.

Ахборотни муҳофаза қилиш соҳасида мувофиқлик сертификациясини ўтказиш учун ўз қоидалари, процедуралари ва бошқарувига эга бўлган тизим.

**Система управления доступом**

Автоматизированные средства физического управления доступом. Например, использо-

## С

**uz** - эркин фойдаланишни бошқариш тизими

**en** - access control system, ACS

вание идентификационных карт с магнитной полосой, смарткарт, считывающих биометрических устройств.

Эркин фойдаланишни жисмоний бошқаришнинг автоматлаштирилган воситалари. Масалан, магнит полосали идентификацион карталардан, ҳисоблайдиган биометрик курилмалардан, смарт-карталардан фойдаланиш.

**Система управления информационной безопасностью**

**uz** - ахборот хавфсизлигини бошқариш тизими

**en** - information security management system

Комплекс мер, направленных на обеспечение режима информационной безопасности на всех стадиях жизненного цикла системы.

Тизим ҳаётий циклининг барча босқичларида ахборот хавфсизлиги режимини таъминлашга қаратилган чора-тадбирлар комплекси.

**Система управления ключами**

**uz** - калитларни бошқариш тизими

**en** - key management system

Составная часть ключевой системы, определяющая порядок использования, смены, хранения и архивирования, резервного копирования и восстановления, замены или изъятия из обращения скомпрометированных, а также уничтожения старых ключей.

Калит тизимининг путур етказилган (обрўсизлантирилган) калитлардан фойдаланиш, уларни алмаштириш, сақлаш ва архивлаш, резерв нусха кўчириш, тиклаш, муомаладан чиқариб ташлаш, шунингдек, эски калитларни йўқ қилиш тартибини белгиловчи таркибий қисми.

**Система установки ключей**

**uz** - калитларни

Составная часть ключевой системы, определяющая алгоритмы и процедуры генерации, распределения, передачи и проверки



тайинлаш тизими  
**en** - key setting  
 system

ключей.

Калит тизимининг калитларни генерациялаш, таксимлаш, бериш ва текшириш алгоритмлари ҳамда процедураларини белгиловчи таркибий қисми.

**Система цифровой подписи**  
**uz** - рақамли имзо тизими  
**en** - digital signature system

Процедура и средства, обеспечивающие получателю гарантию подлинности полученного набора данных и достоверность факта отправки данных именно тем отправителем, от имени которого направлено сообщение.

Олувчига, олинган маълумотлар тўпламининг ҳақиқийлигини ва маълумотларнинг айнан, номидан хабар юборилган жўнатувчи томонидан юборилганлик фактининг ишончлилигини таъминлайдиган процедура ҳамда воситалар.

**Система экспертная**  
**uz** - эксперт тизими  
**en** - expert system

Комплекс программных средств, в основу которого положена интерпретация правил, аккумулирующих знания экспертов по определенной специальности.

Дастурий воситалар комплекси, унинг асосига маълум мутахассислик бўйича экспертлар билимини тўпловчи коидалар талқини киритилган.

**Сканер сетевой**  
**uz** - тармоқ сканери  
**en** - network scanner

Программа, которая осуществляет сбор информации о сети для нахождения компьютеров и программ, потенциально уязвимых к атакам.

Хужумлардан потенциал яхши муҳофазаланмаган дастурлар ва компьютерларни топиш мақсадида тармоқ тўғрисида ахборот тўпловчи дастур.

**Сканер уязвимости программ**  
**uz** - дастурларнинг яхши муҳофазаланмаганлик сканери  
**en** - program vulnerability scanner

Программа, которая осуществляет проверку больших групп компьютеров в сети Интернет в поисках машин, уязвимых к тому или иному конкретному виду атаки.

Хужумнинг у ёки бошқа бир аниқ туридан яхши муҳофазаланмаган машиналарни излаб топиш мақсадида Интернет тармоғида компьютерларнинг катта гуруҳи текширилишини амалга оширадиган дастур.

**Скремблер**  
**uz** - скремблер  
**en** - scrambler

1. Шифровальное средство, предназначенное для защиты информации только от непосредственного прослушивания, просмотра или прочтения.

2. Аналоговый речевой шифратор.

1. Ахборотни фақат бевосита эшитиш, кўриб чиқиш ёки ўқишдан муҳофаза қилиш учун мўлжалланган шифрлаш воситаси.

2. Аналог нутк шифратори.

**Скремблирование**  
**uz** - скремблерлаш  
**en** - scrambling

Простейший способ шифрования, основанный на перемешивании входного потока данных (обычно используется для улучшения синхронизирующих свойств входных данных).

Оддий шифрлаш усули, маълумотларнинг кириш оқимини аралаштиришга асосланган (одатда, кириш маълумотларининг синхронловчи хусусиятларини яхшилаш учун ишлатилади).

**След**  
**uz** - из  
**en** - footprint

Часть избыточного кода, которую можно использовать для выявления случаев нарушения авторского права.

Ортикча коднинг муаллифлик ҳукуки бузилган ҳолларни аниқлашда фойдаланиш мумкин бўлган қисми.

## С

**Слово кодовое  
дополнительное**

**uz** - кўшимча кодли  
сўз

**en** - supplementary  
codeword

**Служба аутенти-  
фикации удален-  
ных пользовате-  
лей по коммути-  
руемым линиям**

**uz** - коммутацияла-  
надиган линиялар  
бўйича олисдаги  
фойдаланувчилар-  
ни аутентификация  
килиш хизмати

**en** - remote authenti-  
cation dial-in user  
service, RADIUS

**Служба безопас-  
ности**

**uz** - хавфсизлик  
хизмати

**en** - security service

**Служба информа-  
ционной безопас-  
ности сети теле-  
коммуникаций  
общего пользова-  
ния**

**uz** - умумий фойда-  
ланишдаги теле-  
коммуникациялар  
тармоғининг ахбо-

Средство аутентификации, представляющее собой кодовое слово, которое запрашивается у пользователя дополнительно после предъявления пароля.

Аутентификация килиш воситаси. Пароль кўрсатилгандан кейин фойдаланувчидан кўшимча равишда сўраладиган кодли сўз.

Протокол, предназначенный для централизованной проверки регистрационных данных пользователей (паролей и т.п.) на сервере аутентификации.

Аутентификация килиш серверида фойдаланувчиларнинг қайд қилинган маълумотларини (пароллар ва ш.к.) марказлаштирилган тарзда текшириш учун мўлжалланган протокол.

Служба, обеспечивающая защиту систем телекоммуникаций и передаваемых данных.

Телекоммуникациялар тизимларининг ва узатиладиган маълумотларнинг муҳофаза қилинишини таъминловчи хизмат.

Организационно-техническая структура сети телекоммуникаций общего пользования, реализующая на базе определенных механизмов информационной безопасности определенные процедуры защиты, направленные на обеспечение информационной безопасности сети телекоммуникаций общего пользования.

Умумий фойдаланишдаги телекоммуника-

## С

роғ хавфсизлиги  
хизмати  
**en** - public switched  
telecommunications  
network information  
security service

**Служба обеспечения информации  
безопасности**

**uz** - ахборот хав-  
фсизлигини  
таъминлаш хизмати  
**en** - information  
security service

**Смарфинг**  
**uz** - смарфинг  
**en** - smurfing

**Сниффинг**  
**uz** - sniffing  
**en** - sniffing

**Собственник информации**  
**uz** - ахборот эгаси

циялар тармоғи ахборот хавфсизлигини таъминлашга йўналтирилган, ахборот хавфсизлигининг белгиланган механизмлари асосида белгиланган муҳофаза процедураларини амалга оширувчи, умумий фойдаланишдаги телекоммуникациялар тармоғининг ташкилий-техник структураси.

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

Ахборот хавфсизлигини таъминлашнинг ташкилий-техник, аппарат-дастурий ва режимли чора-тадбирларини ишлаб чиқиш, амалга ошириш ва назорат қилиш билан шуғулланувчи структуравий бўлинма.

Способ атаки хакеров на сервер провайдера, заключающийся в посылке множества ping-запросов с ложным обратным адресом.

Хакерларнинг провайдер серверига қилдиган хужум усули. Тескари адреси сохта бўлган кўплаб ping сўровларни юборишда ифодаланади.

Прослушивание трафика с целью сбора передаваемых паролей, ключей и другой идентификационной или аутентификационной информации.

Узатиладиган пароллар, қалитлар ва бошқа идентификацион ёки аутентификацион ахборотни тўплаш мақсадида трафикни эшитиш.

1. Субъект, реализующий в полном объеме полномочия владения, пользования, распоряжения информацией в соответствии с

## С

**en** - owner of information

законодательными актами.

2. Субъект информационных отношений, обладающий юридическим правом владения, распоряжения и пользования информационным ресурсом. Юридическое право владения, распоряжения и пользования информационным ресурсом принадлежит лицам, получившим этот информационный ресурс по наследству.

1. Қонунчилик актларига мувофиқ ахборотга эгалик қилиш, фойдаланиш ваколатини тўлик ҳажмда амалга оширувчи субъект.

2. Ахборот муносабатларининг ахборот ресурсига эгалик қилиш, тасарруф этиш ва фойдаланиш юридик ҳуқуқига эга бўлган субъекти. Бундай юридик ҳуқуқ шу ахборот ресурсини мерос бўйича олган шахсга тегишли бўлади.

**Событие**  
**uz** - воқеа  
**en** - event

Появление значимого нормального или отличного от нормального условия.

Аҳамиятли нормалнинг ёки нормал шаритдан фарқ қилувчининг пайдо бўлиши.

**Соглашение об аутентификации и выборе ключей**  
**uz** - калитларни аутентификация қилиш ва танлаш тўғрисида битим  
**en** - Authentication and Key Selction Agreement

Процедура двусторонней аутентификации в 3G-сетях, при которой на передающей стороне формируется аутентификационный вектор и согласуется с приемной стороной. Если соглашение достигнуто, то осуществляется вычисление ключей шифрования и целостности, в противном случае запрос отклоняется.

3G тармоқларида икки томонлама аутентификация қилиш процедураси, бунда узатувчи томонда аутентификацион вектор шаклланади ва қабул қилувчи томон билан келишилади. Агар келишувга эришилса,

## С

шифрлаш калитини ҳисоблаш амалга оширилади, акс ҳолда сўров бекор қилинади.

**Сокрытие**  
**uz** - яшириш  
**en** - hiding  
concealment

Способ технической защиты информации, состоящий в ухудшении условий обнаружения носителей информации и ее получения.

Ахборотни техник муҳофаза қилиш усули бўлиб, ахборот ташувчиларни аниқлаш ва ахборотни олиш шароитларини ёмонлаштиришдан иборат.

**Сообщение**  
**uz** - хабар  
**en** - message

1. Строка битов ограниченной длины  
2. Информация, выраженная в определенной форме и предназначенная для передачи от источника информации к ее получателю с помощью сигналов различной физической природы.

1. Чекланган узунликдаги битлар сатри.  
2. Маълум шаклда ифодаланган ва турли физик табиатга эга бўлган сигналлар ёрдамида ахборот манбаидан уни олувчига уза тиш учун мўлжалланган ахборот.

**Сообщение крипто-стойкое**  
**uz** - криптобардошли хабар  
**en** - crypto-proof message

Сообщение, которое не может быть дешифровано без знания криптографического ключа.

Криптографик калитни билмасдан туриб, дешифровка қилиш мумкин бўлмаган хабар.

**Сообщение одно-разовое**  
**uz** - бир мартали хабар  
**en** - single-shot message

Идентификатор или номер, который используется только один раз, т.е. в каждом последующем сеансе связи его значение обновляется.

Фақат бир марта ишлатиладиган идентификатор ёки рақам, яъни ҳар бир кейинги алоқа сеансида унинг қиймати янгиланади.

## С

- Сообщение с цифровой подписью**  
**uz** - рақамли имзоли хабар  
**en** - digital signature message
- Сообщение, которое не зашифровано, но содержит цифровую подпись.**
- Сообщение, которое не зашифровано, но содержит цифровую подпись.**  
 Шифрланмаган, лекин рақамли имзога эга бўлган хабар.
- Состояние безопасное**  
**uz** - хавфсиз ҳолат  
**en** - secure state
- Условие, при выполнении которого ни один субъект не может получить доступ ни к какому объекту иначе как на основе проверки имеющихся у него полномочий.**
- Состояние безопасности**  
**uz** - хавфсизлик ҳолати  
**en** - security state
- Информация о состоянии, которая хранится в открытой системе и требуется для предоставления услуг безопасности.**
- Состояние санкционированное (разрешенное)**  
**uz** - рухсат этилган ҳолат  
**en** - authorized (allowed) state
- Очиқ тизимда сақланадиган ва хавфсизлик хизматларини тақдим этиш учун талаб этиладиган ҳолат тўғрисидаги ахборот.**
- Состояние, при котором непривилегированная программа имеет доступ к ресурсам, недоступным в других условиях.**
- Состояние, при котором непривилегированная программа имеет доступ к ресурсам, недоступным в других условиях.**  
 Имтиёзга эга бўлмаган дастур бошқа шароитларда эркин фойдаланиш мумкин бўлмаган ресурслардан фойдалана оладиган ҳолат.
- Сохранность данных**  
**uz** - маълумотларнинг яхши сақланганлиги  
**en** - data integrity
- Способность информационной системы обеспечивать в течение своего жизненного цикла хранение данных в неискаженном виде и исключать их случайное уничтожение.**
- Ахборот тизимининг ўз ҳаётий цикли мо-**

## С

байнида маълумотларнинг бузилмаган ҳолда сақланишини ва уларнинг тасодифий равишда йўқ қилинмаслигини таъминлаш хусусияти.

### **Спаминг**

**uz** - спаминг

**en** - spamming

Посылка большого числа одинаковых сообщений в различные группы USENET. Часто используется для организации дешевой рекламной кампании, пирамид или просто для того, чтобы надоест людям.

USENET турли гурухларига бир хил хабарларни кўплаб юбориш. Одатда, арзон реклама кампанияси, пирамидалар ташкил қилиш ёки шунчаки одамларнинг жонига тегиш учун қўлланилади.

### **Список апробированной продукции**

**uz** - маъқулланган

маҳсулот рўйхати

**en** - evaluated products list, EPL

Список оборудования, аппаратуры и программного обеспечения, который было оценен и признан соответствующим определенному классу, согласно стандарту Trusted Computer System Evaluation Criteria (TCSEC).

Trusted Computer System Evaluation Criteria (TCSEC) стандартига мувофиқ, маълум классга мос келади деб баҳоланган ва тан олинган ускуна, аппаратура ва дастурий таъминот рўйхати.

### **Список доступа**

**uz** - эркин фойдаланиш рўйхати

рўйхати

**en** - access list, ACL

Массив записей контроля доступа.

*Примечание: Различают дискреционный список контроля доступа, управляющий доступом пользователей к объекту, и системный список контроля доступа, управляющий аудитом доступа к объекту.*

Эркин фойдаланишни назорат қилиш ёзувларининг массиви.

*Изоҳ: Эркин фойдаланишни назорат қилишнинг дискрецион рўйхати, фойдаланувчиларнинг объектдан эркин фойдаланишини назорат қилиш-*



## С

*нинг тизим рўйхати, объектдан эркин фойдаланиш аудитини бошқарувчи фарқланади.*

### **Список полномочий**

**uz** - ваколатлар рўйхати  
**en** - capabilities list

Ассоциированный с субъектом список, в котором указаны все виды доступа этого субъекта ко всем объектам. Например, для процесса, включенного в список, определены все виды доступа ко всем файлам и другим защищенным ресурсам.

Субъект билан ассоциацияланган, шу субъектнинг ҳамма объектлардан фойдалана олишининг барча турлари кўрсатилган рўйхат. Масалан, рўйхатга киритилган жараён учун барча файллардан ва бошқа ҳимояланган ресурслардан эркин фойдаланишнинг барча турлари аниқланган.

### **Список управления доступом**

**uz** - эркин фойдаланишни бошқариш рўйхати  
**en** - access control list

1. Список логических объектов, имеющих полномочия на получение доступа к ресурсу, вместе с перечнем их прав доступа.
2. Представление матрицы доступа по столбцам – каждому объекту соответствует список субъектов вместе с их правами.

1. Ресурсдан эркин фойдаланиш имкониятини олиш ваколатига эга бўлган мантикий объектларнинг уларнинг фойдалана олиш ҳуқуқлари билан биргаликдаги рўйхати.

2. Эркин фойдаланиш матрицаларини ус-тунлар бўйича тақдим этиш – ҳар бир объектга субъектларнинг рўйхати, уларнинг ҳуқуқлари билан бирга, мос келади.

### **Способ защиты информации**

**uz** - ахборотни муҳофаза қилиш усули  
**en** - information safety methods

Порядок и правила применения определенных принципов и средств защиты информации.

Ахборотни муҳофаза қилишнинг муайян принциплари ҳамда воситаларини қўллаш тартиби ва қоидалари.

## С

**Спуфинг**  
**uz - спуфинг**  
**en - spoofing**

1. Подмена адреса отправителя, реализуемая, как правило, одним из двух способов: либо злоумышленник маскируется под узел внутренней сети, где все узлы – доверенные (т.е. попытка соединения выглядит как запрос внутреннему узлу от другого внутреннего узла), либо под доверенный внешний узел, если не предусмотрено никаких специальных алгоритмов аутентификации.
2. Вид сетевой атаки, при которой злоумышленник пытается войти в защищенную сеть, используя ложный сетевой адрес.
3. Получение доступа путем обмана, т.е. ситуация, когда пользователь пытается соединиться с Интернет-сервером, проху-сервером или межсетевым экраном, используя ложный IP-адрес.

1. Қоидага кўра, иккита усулдан бирида амалга ошириладиган жўнатувчининг адресини алмаштириш: барча узеллар ишончли бўлганда (яъни уланишга уриниш ички узелга бошка ички узелдан сўров сифатида кўринади) ё жинояткор ички тармоқ узели остида никобланади, ёки агар аутентификация қилишнинг ҳеч қандай махсус алгоритмлари кўзда тутилмаган бўлса, ишончли ташқи узел остида никобланади.
2. Тармоқ хужумининг бир тури, бунда жинояткор сохта тармоқ адресидан фойдаланиб, муҳофазаланган тармоққа киришга ҳаракат қилади.
3. Фойдаланувчи сохта IP-адресни ишга солган ҳолда интернет-сервер, проху-сервер ёки тармоқлараро экран билан боғланишга ҳаракат қилганда юзага келадиган вазият.

**Среда безопасная замкнутая**  
**uz - ёпиқ хавфсиз**

Среда, в которой особое внимание уделяется защите данных и ресурсов от случайных или злоумышленных действий (в виде ав-

## С

муҳит  
en - closed-security  
environment

торизации, категорий допусков, управления конфигурацией и т.д).

Маълумотлар ва ресурсларни тасодифий ёки қасдан қилинадиган ҳаракатлардан (муаллифлик, рухсат бериш категориялари, конфигурацияни бошқариш ва ҳ.к. кўри-нишда) муҳофаза қилишга алоҳида эътибор бериладиган муҳит.

**Среда безопасная  
открытая**  
uz - очик хавфсиз  
муҳит  
en - open-security  
environment

Среда, в которой защита данных и ресурсов от случайных или злоумышленных действий достигается посредством нормальных операционных процедур.

Маълумотлар ва ресурсларни тасодифий ёки қасдан қилинадиган ҳаракатлардан муҳофаза қилишга нормал операцион процедуралар воситасида эришиладиган муҳит.

**Среда личной  
безопасности**  
uz - шахсий хав-  
фсизлик муҳити  
en - personal secu-  
rity environment,  
PSE

Безопасное местное хранилище для личного ключа объекта, ключа органа сертификации, пользующегося непосредственным, доверием, и возможно, других данных.

*Примечание: В зависимости от политики обеспечения безопасности объекта или требований к системе эта среда может быть, например, криптографически защищенным файлом или маркером аппаратных средств, защищённых от умышленных повреждений.*

Объектнинг шахсий қалити сақланадиган хавфсиз маҳаллий жой, бевосита ишонч қозонган сертификатлаш органининг қалити ва мумкин бўлган бошқа маълумотлар.

*Изоҳ: Объект хавфсизлигини таъминлаш сис-темасига ёки тизимга қўйиладиган талабларга боғлиқ равишда, бу муҳит, масалан, криптогра-фик муҳофазаланган файл ёки қасдан шикаст-лашлардан муҳофазаланган аппарат воситалар маркери бўлиши мумкин.*

## С

### **Среда с защитой целостности**

**uz** - яхлитлик муҳофаза қилинган муҳит

**en** - integrity-protected environment

Среда, в которой предотвращаются или обнаруживаются несанкционированные изменения данных (включая создание и удаление).

Маълумотларнинг рухсат этилмаган тарзда ўзгартирилиши (жумладан, яратилиши ва чиқариб ташланиши)нинг олди олинадиган ёки аниқланадиган муҳит.

### **Средства защиты информации**

**uz** - ахборотни муҳофаза қилиш воситалари  
**en** - data protection facilities

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

Ахборотни муҳофаза қилиш учун мўлжалланган техник, криптографик, дастурий ва бошқа воситалар, улар амалга оширилган воситалар, шунингдек, ахборотни муҳофаза қилиш самарадорлигини назорат қилиш воситалари.

### **Средства защиты информации законодательные**

**uz** - ахборотни муҳофаза қилишнинг қонунчилик воситалари  
**en** - legislative data protection facilities

Законодательные акты страны, которые регламентируют правила использования, обработки и передачи информации ограниченного доступа и устанавливают меры ответственности за нарушение этих правил.

Мамлакатнинг эркин фойдаланиш чекланган ахборотдан фойдаланиш, уларни қайта ишлаш ва узатиш қоидаларини қатъий тартибга соладиган ва бу қоидаларнинг бузилганлиги учун жавобгарлик чораларини белгилайдиган қонунчилик актлари.

### **Средства защиты информации организационные**

**uz** - ахборотни

Организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации сети телекоммуникаций для обеспечения

## С

муҳофаза қилиш-  
нинг ташкилий  
воситалари  
**en** - organizational  
data protection facili-  
ties

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

Ахборотнинг муҳофаза қилинишини таъминлаш мақсадида телекоммуникациялар тармоқларини яратиш ва улардан фойдаланиш жараёнида амалга ошириладиган ташкилий-техник ва ташкилий-ҳуқуқий тадбирлар. Ташкилий тадбирлар улар ҳаёт циклининг барча босқичларида (лойиҳалаш, синов ва эксплуатация қилиш) тармоқнинг барча структура элементларини қамраб олади.

**Средства защиты информации технические (аппаратно-программные)**

**uz** - ахборотни муҳофаза қилиш техник (аппаратдастурий) воситалари

**en** - technical (hardware and software) data protection facilities

Различные электронные устройства и специальные программы, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

Ахборотни муҳофаза қилиш функцияларини (фойдаланувчиларни идентификациялаш ва аутентификация қилиш, ресурслардан эркин фойдаланишни чеклаш, воқеаларни қайд қилиш, ахборотни криптографик беркитиш ва б.қ.) (мустақил ёки бошқа воситалар билан биргаликда) бажарадиган турли хил электрон қурилмалар ва махсус дастурлар.

**Средства защиты программного обеспечения**  
**uz** - дастурий

Средства, обеспечивающие защиту программных средств от несанкционированного доступа.

таъминотни  
муҳофаза қилиш  
воситалари  
**en** - Software  
protection facilities

**Средства защиты  
физические**  
**uz** - жисмоний  
муҳофаза  
қилиш воситалари  
**en** - physical  
protection facilities

**Средства крипто-  
графические**  
**uz** - криптографик  
воситалар  
**en** - cryptographic  
facilities

Дастурий воситаларнинг рухсат этилмаган тарзда фойдалана олишдан муҳофаза қилиниши таъминлайдиган воситалар.

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.*

Жинояткорнинг сукулиб кириши ва фойдалана олиши мумкин бўлган йўлларда жисмоний тўсиқларни яратиш учун махсус мўлжалланган автоном қурилма ва тизимлар.

*Изоҳ: Аппаратура жойлашган эшиклардаги қулфлар, деразадаги панжаралар, қўриқлаш сигнализациясининг электрон механик ускунаси жисмоний муҳофаза қилиш воситалари бўлиши мумкин.*

1. Методы и средства обеспечения безопасности информации, использующие криптографические преобразования информации.  
2. Средства, реализованные в виде документов, механических, электромеханических, электронных технических устройств или программ, предназначенных для выполнения функций криптографической системы.

1. Ахборотни криптографик ўзгартиришлардан фойдаланиладиган, ахборот хавфсизлигини таъминлашнинг метод ҳамда воситалари.

2. Криптографик тизим функцияларини

## С

бажариш учун мўлжалланган ҳужжатлар, механик, электромеханик, электрон техник қурилмалар ёки дастурлар кўринишидаги воситалар.

**Средства технические вспомогательные**

**uz** - ёрдамчи техник воситалар  
**en** - support technology

Средства и системы формирования, передачи, приема, преобразования, отображения и хранения открытой информации, средства и системы жизнеобеспечения различного назначения, которые могут создавать технические каналы утечки информации.

Очиқ ахборотни шакллантириш, узатиш, қабул қилиш, ўзгартириш, акс эттириш ва сақлаш воситалари ҳамда тизимлари, ахборот чиқиб кетиши мумкин бўлган техник каналлар яратадиган, турли мақсадлардаги ҳаётни таъминлаш тизимлари ва воситалари.

**Средства технические основные**

**uz** - асосий техник воситалар  
**en** - general technical facilities

Средства и системы формирования, передачи, приема, преобразования, отображения и хранения информации с ограниченным доступом.

Эркин фойдаланилиши чекланган ахборотни шакллантириш, узатиш, қабул қилиш, ўзгартириш, акс эттириш ва сақлаш воситалари ҳамда тизимлари.

**Средства технической защиты информации**

**uz** - ахборотни техник муҳофаза қилиш воситалари  
**en** - technical data protection facilities

Технические средства, предназначенные для предотвращения утечки информации по одному или нескольким техническим каналам.

Битта ёки бир нечта техник канал орқали ахборот чиқиб кетишининг олдини олишга мўлжалланган техник воситалар.

**Средства управления доступом**  
**uz** - эркин фойдала-

Средства, предотвращающие случайный или преднамеренный доступ к данным.

нишни бошқариш  
воситалари  
en - access control  
facilities

**Средство вычислительной техники**

uz - ҳисоблаш техникаси воситаси  
en - computer facilities

Маълумотлардан тасодифан ёки касдан  
фойдалана олишни бартараф этувчи воситалар.

1. Техническое средство обработки информации, в котором информация представлена в цифровом коде.

*Примечание: К средствам вычислительной техники относятся процессоры, каналы селективные и мультиплексные, внешние запоминающие устройства, устройства ввода и вывода данных, устройства непосредственной связи оператора с ЭВМ, устройства систем телеобработки данных, устройства повышения достоверности и т.д.*

2. Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

1. Ахборот рақамли кодда тақдим этилган ахборотни қайта ишлаш техник воситаси.

*Изоҳ: Процессорлар, селектив ҳамда мультиплекс каналлар, ташиқ хотирловчи қурилмалар, маълумотларни киритиш ва чиқариш қурилмалари, операторнинг электрон ҳисоблаш машинаси билан бевосита боғланиш қурилмалари, маълумотларни телеқайта ишлаш тизимларининг қурилмалари, шонччиликни ошириш қурилмалари ва бошқа қурилмалар ҳисоблаш техникаси воситаларига тегишлидир.*

2. Мустақил равишда ёки бошқа тизимлар таркибида ишлай оладиган маълумотларни қайта ишлаш тизимлари дастурий ва техник элементларининг жами.

**Средство вычислительной техники (СВТ) защищенное**  
uz - муҳофазалан-

Средство вычислительной техники, в котором реализован комплекс средств защиты.

Муҳофаза қилиш воситаларининг комплекси амалга оширилган ҳисоблаш техникаси



ган ҳисоблаш тех-  
никаси воситаси  
en - protected  
computer facilities

воситаси.

Средство защиты  
uz - муҳофаза  
қилиш воситаси  
en - protection  
facilities

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.

Турли хавфсизлик даражасига эга бўлган иккита маълумотларни қайта ишлаш тизими ўртасида ёки фойдаланувчи терминали ва маълумотлар базаси ўртасида ҳимоя филтри сифатида фойдаланиладиган ҳамда фойдаланувчида улардан эркин фойдаланиш вақолати бўлмаган маълумотларни саралаш учун мўлжалланган функционал блок.

Средство защиты  
информации  
uz - ахборотни  
муҳофаза қилиш  
воситаси  
en - information  
security products

Техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации.

Ахборотни муҳофаза қилиш самарадорлигини назорат қилиш учун мўлжалланган ёки ишлатиладиган техник, дастурий восита, буюм ва/ёки материал.

Средство защиты  
информации ак-  
тивное  
uz - актив ахборот-  
ни муҳофаза қилиш  
воситаси

Средство, обеспечивающее создание активных помех, исключаяющих или существенно снижающих возможность использования канала утечки информации.

Ахборот чиқиб кетиши мумкин бўлган ка-

## С

**en** - active information security product

налдан фойдаланиш имкониятини йўқка чиқарадиган ёки жиддий равишда камайтирувчи актив халакитлар вужудга келтирилишини таъминлайдиган восита.

**Средство защиты информации аппаратное**

**uz** - ахборотни муҳофаза қилишнинг аппарат воситаси

**en** - information security hardware

1. Механические, электромеханические, электронные, оптические, лазерные, радио, радиотехнические, и другие устройства, системы и сооружения, предназначенные для защиты информации от несанкционированного доступа, копирования, кражи, модификации или разрушения.

2. Специальное защитное устройство или приспособление, входящее в комплект технического средства обработки информации.

1. Ахборотни рухсат этилмаган тарзда фойдаланиш, нухса кўчириш, ўғирлаш, ўзгартириш ёки бузишдан муҳофаза қилиш учун мўлжалланган механик, электромеханик, электрон, оптик, лазер, радио, радиотехник ва бошқа қурилмалар, тизимлар ва иншоотлар.

2. Махсус химоя қурилмаси ёки ахборотни қайта ишлаш техник воситасининг комплектига қирувчи мослама.

**Средство защиты информации программное**

**uz** - ахборотни муҳофаза қилиш дастурий воситаси

**en** - information security software

Специальная программа, входящая в комплект программного обеспечения и предназначенная для защиты информации.

Дастурий таъминот комплектига қирувчи ва ахборотни муҳофаза қилиш учун мўлжалланган махсус дастур.

**Средство защиты информации техническое**

**uz** - ахборотни муҳофаза қилиш

1. Техническое средство, предназначенное для устранения или ослабления демаскирующих признаков объекта, создания ложных (имитирующих) признаков, а также помех техническим средствам доступа ин-

## С

нинг техник воситаси  
**en** - technical information security equipment

формации.

2. Специальные средства (устройства), предназначенные для предотвращения противоправных действий с информацией и/или обеспечения охраны (физической защиты) объекта защиты.

1. Объектнинг демаскировкаловчи аломатларини бартараф қилиш ёки сусайтириш, сохта (имитацияловчи) аломатларни, шунингдек, ахборотдан эркин фойдаланиш техник воситаларига халақитлар вужудга келтириш учун мўлжалланган техник восита.

2. Ахборот билан боғлиқ бўлган қонунга ҳилоф ишларнинг олдини олиш ва/ёки муҳофаза объектнинг қўриқланишини (жисмоний ҳимоя қилинишини) таъминлаш учун мўлжалланган махсус воситалар (қурилмалар).

**Средство защиты от несанкционированного доступа**  
**uz** - рухсат этилмаган тарзда эркин фойдаланишдан муҳофаза қилиш воситаси  
**en** - unauthorized access protection facility

Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

Рухсат этилмаган тарзда фойдаланишнинг олдини олиш ёки жиддий равишда қийинлаштириш учун мўлжалланган дастурий, техник ёки дастурий-техник восита.

**Средство контроля эффективности защиты информации**  
**uz** - ахборотни муҳофаза қилиш самарадорлигини назорат қилиш во-

Техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации.

Ахборотни муҳофаза қилиш самарадорлигини назорат қилиш учун мўлжалланган ёки фойдаланиладиган техник, дастурий

## С

ситаси

**en** - information security efficiency control facility

**Средство криптографической защиты информации**

**uz** - ахборотни криптографик муҳофаза қилиш воситаси

**en** - cryptographic information protection facility

**Средство обработки информации техническое**

**uz** - ахборотни қайта ишлаш техник воситаси

**en** - information processing hardware

восита, модда ва/ёки материал.

Аппаратное, программное или аппаратно-программное средство, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Ахборот хавфсизлигини таъминлаш мақсадида, ахборотнинг криптографик ўзгартирилишини амалга оширувчи аппарат, дастурий ёки аппарат-дастурий восита.

Техническое средство, предназначенное для приема, хранения, поиска, преобразования, отображения и/или передачи информации по каналам телекоммуникаций.

*Примечание: К техническим средствам обработки информации относятся средства вычислительной техники, средства и системы телекоммуникаций, средства записи, усиления и воспроизведения звука, переговорные и телевизионные устройства, средства изготовления и размножения документов, кинопроекционная аппаратура и другие технические средства, связанные с приемом, накоплением, хранением, поиском, преобразованием, отображением и/или передачей информации по каналам телекоммуникаций.*

Телекоммуникация каналлари орқали ахборотни қабул қилиш, сақлаш, излаш, ўзгартириш, акс эттириш ва/ёки узатиш учун мўлжалланган техник восита.

*Изоҳ: Ахборотни қайта ишлаш техник воситаларига ҳисоблаш техникаси воситалари, телекоммуникация тизимлари ва воситалари, овоз ёзиш, қучайтириш ва қайта эшиттириш воситалари, сўзлашув ва телевизион қурilmалар,*

*хужжатлар тайёрлаш ва кўпайтириш воситалари, кинопроектор аппаратура ҳамда телекоммуникациялар каналлари орқали ахборот қабул қилиш, тўплаш, сақлаш, излаш, ўзгарттириш, акс эттириш ва ёки узатиш билан боғлиқ бўлган бошқа техник воситалар қиради.*

**Средство разграничения доступа**  
**uz** - эркин фойдаланишни чегаралаш воситаси  
**en** - access isolation facility

Программно-аппаратное средство, обеспечивающее разграничение доступа субъектов к информационным ресурсам в соответствии с принятой моделью.

*Примечание: Средствами разграничения доступа являются матрица доступа и метка секретности (конфиденциальности).*

Қабул қилинган моделга мувофиқ субъектларнинг ахборот ресурсларидан эркин фойдаланиши чегараланишини таъминловчи дастурий-аппарат восита.

*Изоҳ: Фойдаланиш матричаси ва махфийлик (конфиденциаллик) белгиси эркин фойдаланишни чегаралаш воситалари ҳисобланади.*

**Средство шифровальное**  
**uz** - шифрловчи восита  
**en** - encryption facility

1. Реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для защиты информации, циркулирующей в технических средствах, при ее обработке, хранении и передаче по каналам телекоммуникаций, включая шифровальную технику.

2. Аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для изготовления и распределения ключевых документов, используемых в шифровальных средствах, независимо от вида носителя ключевой информации.

3. Аппаратные, программные и аппаратно-программные средства, системы и комплексы,

## С

сы защиты от навязывания ложной информации, включая средства имитозащиты и электронной подписи, реализующие криптографические алгоритмы преобразования информации.

1. Ахборотни ўзгартиришнинг криптографик алгоритмларини амалга оширадиган аппарат, дастурий, аппарат-дастурий воситалар, техник воситаларда айланадиган ахборотни, уни қайта ишлаш, сақлаш ва телекоммуникациялар каналлари орқали узатиш пайтида муҳофаза қилиш учун мўлжалланган тизим ҳамда комплекслар, жумладан, шифрлаш техникаси.

2. Қалитли ахборотни ташувчининг туридан қатъи назар, шифрлаш воситаларида фойдаланиладиган қалитли хужжатларни тайёрлаш ва тарқатиш учун мўлжалланган аппарат, дастурий, аппарат-дастурий воситалар, тизим ва комплекслар.

3. Сохта ахборотни мажбуран киритилишидан (қабул қилинишидан) муҳофаза қилишнинг аппарат, дастурий ва аппарат-дастурий воситалари, тизимлари ва комплекслари, жумладан, ахборотни ўзгартиришнинг криптографик алгоритмларини амалга оширувчи, имитомуҳофаза ва электрон имзо воситалари.

**Стеганография**  
uz - стеганография  
en - steganography

Отрасль науки, изучающая математические методы сокрытия конфиденциальной информации в открытых информационных массивах.

Очик ахборот массивларида конфиденциал ахборотни яширишнинг математик методларини ўрганувчи фан соҳаси.

**Стеганография**

Сокрытие сообщения или файла в другом

## С

- компьютерная уз** - компьютер стеганографияси  
**en** - computer stenography
- Стегоканал уз** - стегоканал  
**en** - stegochannel
- Стегоключ уз** - стегокалит  
**en** - stegokey
- Стегоконтейнер уз** - стегоконтейнер  
**en** - stegocontainer
- Стойкость криптографическая уз** - криптографик бардошлилик  
**en** - cryptoresistability
- Стратегия защиты уз** - муҳофаза қилиш стратегияси  
**en** - protection strategy
- сообщении или файле.
- Хабар ёки файли бошқа хабар ёки файлда яшириш.
- Канал скрытой передачи информации.
- Ахборотни яширин узатиш канали.
- Секретный ключ, необходимый для скр-тия (шифрования) информации.  
 Ахборотни яшириш (шифрлаш) учун зарур бўладиган махфий калит.
- Контейнер, содержащий встроенное сообще-ние.
- Киритилган хабар бўлган контейнер.
- Способность криптосистемы противостоять попыткам криптоаналитика дешифровать шифротекст, раскрыть ключи шифра или нарушить целостность и/или подлинность информации.
- Криптотизимнинг криптоаналитикнинг шифр матни дешифровка қилиш, шифр калитини очиш ёки ахборот яхлитлигини ва/ёки ҳақиқийлигини бузишга бўлган ури-нишларига қарши тура олиш қобилияти.
- Формальное определение критериев, осо-бенно оперативных, которыми следует ру-ководствоваться при обеспечении защиты системы от известных угроз.
- Тизимнинг маълум таҳдидлардан муҳофаза қилинишини таъминлашда амал қилиниши керак бўлган критерийларни, айниқса, опе-ратив критерийларни расмий аниқлаш.

## С

### Субключ

uz - субкалит

en - subkey

Ключ, который включается в состав главного ключа и который можно в любой момент аннулировать без последствий для главного ключа.

Асосий калит таркибига киритиладиган ва исталган вақтда асосий калит учун салбий оқибатларсиз бекор қилиниши мумкин бўлган калит.

### Субъект

uz - субъект

en - subject

1. Активный логический объект, имеющий доступ к объектам. Например, процесс, который запускает выполнение программы.

*Примечание: Субъект может быть причиной потока информации между объектами или изменения состояния системы обработки данных.*

2. Активный компонент системы, обычно представленный в виде пользователя, процесса или устройства, который может явиться причиной потока информации от объекта к объекту или изменения состояния системы. Обычно субъект представляется парой процесс – домен.

3. Активная сущность (процесс, пользователь, устройство и т.д.), вызывающая образование информационного потока между объектами или изменения состояния системы.

1. Объектлардан фойдалана олиш имконияти бўлган мантиқий актив объект. Масалан, дастур бажарилишини ишга туширадиган жараён.

*Изоҳ: Субъект объектлар ўртасидаги ахборот оқимининг ёки маълумотларни қайта ишлаш тизими ҳолати ўзгаришининг сабабчиси бўлиши мумкин.*

2. Одатда, фойдаланувчи, жараён ёки қурилма кўринишида такдим этилган тизимнинг актив компоненти, у объектдан объектга боладиган ахборот оқимининг ёки тизим ҳолати



## С

Ўзгаришининг сабабчиси бўлиши мумкин. Одатда, субъект жараён домен жуфти тарзида тақдим этилади.

3. Объектлар ўртасида ахборот оқими ҳосил қилувчи ёки тизим ҳолатини ўзгартирувчи актив моҳият (жараён, фойдаланувчи, қурилма ва ҳ.к.).

**Субъект безопасности**

**uz** - хавфсизлик

субъекти

**en** - security subject

Активная системная составляющая, к которой применяется политика безопасности.

Хавфсизлик сиёсати татбиқ қилинадиган актив тизим ташкил этувчиси.

**Субъект доступа**

**uz** - эркин фойдаланиш субъекти

**en** - access subject

1. Лицо или процесс, действия которых регламентируются правилами разграничения доступа.

2. Лицо или процесс, осуществляющие доступ к информационному ресурсу с использованием штатных технических средств.

1. Ҳаракатлари фойдалана олишни чегаралаш қоидалари билан қатъий тартибга солинадиган шахс ёки жараён.

2. Штат техник воситалар ёрдамида ахборот ресурсидан эркин фойдаланишни амалга оширувчи шахс ёки жараён.

**Субъект доступа авторизованный**

**uz** - муаллифлаштирилган эркин

фойдаланиш субъекти

экти

**en** - authorized

access subject

Субъект, которому предоставлены соответствующие права доступа к объектам системы (полномочия).

Тизим объектларидан эркин фойдаланиш юзасидан тегишли ҳуқуқлар (ваколатлар) тақдим этилган субъект.

**Субъекты информационных отношений**

**uz** - ахборот муно-

Государство, государственные органы, государственные, общественные или коммерческие организации (объединения) и предприятия (юридические лица), отдельные

## С

сабатларининг  
субъектлари  
en - parties of infor-  
mation relationships

граждане (физические лица) и иные субъекты, взаимодействующие с целью совместной обработки информации.

*Примечание: По отношению к информации, обрабатываемой в информационной системе, различные субъекты – участники информационных отношений могут выступать (возможно, одновременно) в качестве:*

- источников информации;
- пользователей (потребителей) информации;
- собственников (владельцев, распорядителей) информации;
- физических и юридических лиц, о которых собирается и обрабатывается информация;
- владельцев информационной системы и участников процессов обработки и передачи информации и т.д.

Ахборотни биргаликда қайта ишлаш мақсадида ўзаро ҳамкорлик қилувчи давлат, давлат органлари, давлат, жамоат ёки тижорат ташкилотлари (бирлашмалари) ва корхоналар (юримдик шахслар), айрим фуқаролар (жисмоний шахслар) ва бошқа субъектлар.

*Изоҳ: Ахборот тизимида қайта ишланадиган ахборотга нисбатан, турли субъектлар – ахборот муносабатлари иштирокчилари сифатида чиқишлари (балки, бир вақт-да) мумкин:*

- ахборот манбалари;
- ахборот фойдаланувчилари (истеъмолчилари);
- ахборот эгалари;
- ахборот тўпланадиган ва қайта ишланадиган жисмоний ва юримдик шахслар;
- ахборот тизими эгалари ва ахборотни қайта ишлаш ва узатиш жараёнларининг иштирокчилари ва ҳ.к.

Сумма контрольная  
uz - назорат суммаси

1. Информация, предназначенная для проверки правильности записи данных путем подсчета суммы байтов и добавления ее к записи. При считывании данных сумма

## С

**en - checking sum** байтов должна совпасть с контрольной суммой.

2. Некоторая функция, сопоставляемая блоку данных для целей проверки, обычно формируется в виде суммы соответствующих полей всех записей файла. Это число не имеет какого-то особого смысла, а служит только для проверки записей файла. Всякое изменение значения поля обнаруживается из-за несовпадения зарегистрированной ранее и вновь вычисленной контрольных сумм.

1. Байтлар суммасини ҳисоблаш ва уни ёзувга кўшиш йўли билан маълумотлар ёзувининг тўғрилигини текшириш учун мўлжалланган ахборот. Маълумотларни ҳисоблашда байтлар суммаси назорат суммаси билан мос келиши керак.

2. Маълумотлар блокига текшириш мақсадларида солиштириладиган қандайдир функция, одатда файлнинг барча ёзувлари майдонларига мос келувчи сумма кўринишида шаклланади. Бу сон бирор-бир муҳим маънога эга эмас, фақат файл ёзувларини текшириш учун хизмат қилади. Майдон қийматининг ҳар қандай ўзгариши олдиндан қайд қилинган ва қайтадан ҳисобланган назорат суммаларининг мос келмаслигидан аниқланади.

**Суперсектор**  
**uz - суперсектор**  
**en - supersector**

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

Нусха кўчиришдан муҳофаза қилиш методининг қисми. Диска одатдагидан катта ўлчамлардаги сектор ёзилганда қўлланилади.

## С

### **Схема концептуальная**

**uz** - концептуал  
схема

**en** - conceptual  
scheme

Описание возможных состояний связей в предметной области, включая классификации, правила, законы и т.п., действующие между объектами в пределах предметной области.

Предмет соҳаси доирасида объектлар ўртасида амал қилувчи классификациялар, қонунлар ва ш.к. ўз ичига олган ҳолда предмет соҳасидаги алоқалар мумкин бўлган ҳолатларнинг тавсифи.

### **Схема предварительного распределения ключей**

**uz** - қалитларни  
олдиндан тақсимлаш  
схемаси

**en** - preliminary key  
distribution scheme

Совокупность алгоритма распределения исходной ключевой информации и алгоритма формирования ключей.

Бошланғич қалит аҳборотни тақсимлаш ва қалитларни шакллантириш алгоритмларининг жами.

### **Схема цифровой подписи**

**uz** - рақамли имзо  
схемаси

**en** - digital signature  
scheme

Совокупность алгоритма формирования цифровой подписи и алгоритма ее проверки.

Рақамли имзони шакллантириш ва уни текшириш алгоритмларининг жами.

### **Сцепление криптографическое**

**uz** - криптографик  
илашиш

**en** - cryptographic  
chaining

Режим использования криптографического алгоритма, при котором преобразование осуществляется алгоритмом, который зависит от значений предыдущих входных или выходных данных.

Криптографик алгоритмдан фойдаланиш режими, бунда ўзгартириш олдинги кириш ёки чиқиш маълумотлари қийматларига боғлиқ бўлган алгоритм томонидан амалга оширилади.

### **Счетчик команд**

Внутренний регистр процессора, содержа-

## С

**uz** - командаларни  
хисоблагич  
**en** - program counter  
control counter

ший адрес следующей выбираемой команды либо следующего байта (слова) программы.

Процессорнинг навбатдаги танланадиган команда адресини ёки дастурнинг навбатдаги байти (сўзи)ни ичига оладиган ички регистри.

## Т

**Тайна коммерческая**

**uz** - тижорат сирини  
**en** - commercial  
confidentiality

Сведения конфиденциального характера из любой сферы деятельности государственного или частного предприятия, разглашение которых может нанести материальный или моральный ущерб ее владельцам или пользователям (юридическим лицам). Охрана коммерческой тайны осуществляется ее владельцем.

Давлат ёки хусусий корхона фаолиятининг исталган соҳасидаги конфиденциал характердаги маълумотлар, уларнинг тарқатилиши эгалари ёки фойдаланувчиларига (юридик шахсларга) моддий ёки маънавий зарар етказиши мумкин. Тижорат сирини сақлаш унинг эгаси томонидан амалга оширилади.

**Текст зашифрованный**

**uz** - шифрланган  
матн  
**en** - ciphertext

Текст или иной вид сообщений, структура которого преобразована с использованием криптографических алгоритмов.

Структураси криптографик алгоритмлардан фойдаланиб ўзгартирилган матн ёки хабарларнинг бошқа тури.

**Текст открытый**

**uz** - очик матн  
**en** - plaintext

1. Данные, семантическое содержимое которых доступно без использования криптографических методов.

2. Исходное защищаемое сообщение.

3. Сообщение, поступающее на вход устройства шифрования или считываемое с выхода приемника после дешифрования.

1. Семантик таркибини криптографик методлардан фойдаланмасдан билиш мумкин бўлган маълумотлар.

2. Дастлабки муҳофаза қилинадиган хабар.

3. Шифрлаш қурилмасининг киришига келиб тушадиган ёки шифрлашдан сўнг қабул қилгичнинг чиқишида ҳисобланадиган хабар.

### **Тестирование на проникновение**

**uz** - суқулиб киришга тестлаш  
**en** - penetration testing

Исследование функций системы обработки данных с целью поиска способов обхода компьютерной безопасности.

Компьютер хавфсизлигини четлаб ўтиш усуллари излаб топиш мақсадида маълумотларни қайта ишлаш тизими функцияларини тадқиқ этиш.

## **У**

### **Угроза**

**uz** - таҳдид  
**en** - threat

1. Потенциальная возможность нарушения компьютерной безопасности.

2. Любые обстоятельства или события, которые могут являться причиной нанесения ущерба системе в форме разрушения, раскрытия или модификации данных, и/или отказа в обслуживании.

3. Любое действие или событие, которое потенциально может привести к нарушению безопасности системы.

1. Компьютер хавфсизлиги бузилишининг потенциал имконияти.

2. Маълумотларни бузиш, очиш ёки ўзгартириш ва/ёки хизмат кўрсатишни рад этиш шаклида тизимга зарар етказиш сабабчиси ҳисобланиши мумкин бўлган ҳар қандай ҳолат ёки воқеа.

## У

3. Потенциал равишда тизим хавфсизлигининг бузилишига олиб келиши мумкин бўлган ҳар қандай ҳаракат ёки воқеа.

**Угроза автоматизированной системы**

**uz** - автоматлаштирилган тизимга таҳдид

**en** - automated system treat

Потенциально возможное событие, действие, процесс или явление, которые могут привести к нанесению ущерба (материального, морального или иного) ресурсам автоматизированной системы.

Автоматлаштирилган тизим ресурсларига (моддий, маънавий ёки бошқа) зарар келтириши мумкин бўлган потенциал воқеа, ҳаракат, жараён ёки ҳодиса.

**Угроза активная**

**uz** - актив таҳдид

**en** - active threat

1. Любая угроза преднамеренного несанкционированного изменения состояния системы обработки данных. Например, угроза, в результате реализации которой возможны модификация сообщений, вставка ложных сообщений, маскарад или отказ в обслуживании.

2. Угроза преднамеренного несанкционированного изменения состояния функционирования системы или сети телекоммуникаций.

1. Маълумотларни қайта ишлаш тизими ҳолатини қасддан рухсат этилмаган тарзда ўзгартиришга бўлган ҳар қандай таҳдид. Масалан, амалга оширилиши натижасида хабарларнинг ўзгартирилиши, ёлғон хабарларнинг киритилиши, алдамчилик ёки хизмат кўрсатишнинг рад этилиши мумкин бўладиган таҳдид.

2. Телекоммуникациялар тизимлари ёки тармоқнинг ишлаш ҳолатини қасддан рухсат этилмаган тарзда ўзгартиришга бўлган таҳдид.

**Угроза безопасности****uz** - хавфсизликка таҳдид**en** - security threat

Возможная опасность (потенциальная или реально существующая) совершения какого-либо действия, направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и потери информации.

Ахборотнинг бузиб кўрсатилиши ва йўқолиш хавфи бўлишида кўринадиган, мулкдорга ёки фойдаланувчига зарар етказадиган, муҳофаза объектига (ахборот ресурсларига) қарши йўналтирилган қандайдир ҳаракатни амалга оширишнинг мумкин бўлган (потенциал ёки реал мавжуд) хавфи.

**Угроза безопасности информации****uz** - ахборот хавфсизлигига таҳдид**en** - data security treat

1. Потенциально возможное событие, действие, процесс или явление, которые могут привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию.

2. Совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее.

1. Ахборотнинг конфиденциаллиги, яхлитлиги, ундан фойдалана олишлик бузилишига, шунингдек, унинг ғайриқонуний тарзда кўпайтирилишига олиб келиши мумкин бўлган потенциал воқеа, ҳаракат, жараён ёки ходиса.

2. Ахборотнинг тарқатилиши ва/ёки унга рухсат этилмаган тарзда ва/ёки кўзда тутилмаган таъсирлар билан боғлиқ потенциал ёки мавжуд реал хавфни вужудга келтирувчи шароитлар ва омиллар жами.



**Угроза интересам субъектов информационных отношений**

**uz** - ахборот муносабатлари субъектларининг манфаатларига таҳдид

**en** - treat towards the interests of information relapses subjects

Потенциально возможное событие, действие, процесс или явление, которые посредством воздействия на информацию и другие компоненты автоматизированной системы могут привести к нанесению ущерба интересам данных субъектов.

Ахборотга ва автоматлаштирилган тизимнинг бошқа компонентларига таъсир этиш орқали берилган субъектларнинг манфаатларига зарар келтириши мумкин бўлган потенциал воқеа, ҳаракат, жараён ёки ходиса.

**Угроза информационной**

**uz** - информация таҳдид

**en** - information treat

Фактор или совокупность факторов, создающих опасность нарушения свойств информации.

Ахборот хусусиятларининг бузилиш хавфини вужудга келтирувчи омил ёки омиллар йиғиндиси.

**Угроза информационной безопасности инфокоммуникационной системы**

**uz** - ахборот-коммуникация тизими ахборот хавфсизлигига таҳдид

**en** - treat towards infocommunication system information security

Действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию ресурсов сети.

Тармоқ ресурсларини бузиш, бузиб кўрсатиш ёки улардан рухсат этилмаган тарзда фойдаланишга олиб келиши мумкин бўлган ҳаракат ёки воқеа.

**Угроза информационной безопасности сети телекоммуникаций общего поль-**

Предполагаемое воздействие злоумышленника на сеть телекоммуникаций общего пользования, непредотвращение, необнаружение и неликвидация которого средст-

**зования**

**uz** - умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавфсизлигига таҳдид

**en** - public switched telecommunications network information security threat

вами сети может привести к снижению заданного уровня обеспечения информационной безопасности сети телекоммуникаций общего пользования.

Умумий фойдаланишдаги телекоммуникациялар тармоғига жинояткорнинг кўзда тутилган таъсири, унинг тармоқ воситалари билан бартараф қилинмагани, аниқланмагани ва йўқ қилинмагани умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавфсизлигини таъминлашнинг берилган даражаси пайсийшига олиб келиши мумкин.

**Угроза пассивная**

**uz** - пассив таҳдид  
**en** - passive threat

1. Угроза несанкционированного раскрытия содержания информации без изменения состояния системы обработки данных. Например, угроза, в результате реализации которой возможно восстановление чувствительной информации из перехваченных передаваемых данных.

2. Возможность несанкционированного доступа к информации без изменения режима функционирования системы.

1. Ахборот мазмунини рухсат этилмаган тарзда, маълумотларни қайта ишлаш тизими ҳолатини ўзгартирмасдан очишга бўлган таҳдид. Масалан, шундай таҳдидки, уни амалга ошириш натижасида қўлга киритилган узатиладиган маълумотлардан таъсирчан ахборотни тиклаш мумкин бўлади.

2. Тизимнинг ишлаш режимини ўзгартирмасдан ахборотдан рухсат этилмаган тарзда фойдалана олиш имконияти.

**Угроза физическая**

**uz** - физик таҳдид  
**en** - physical threat

Угроза, последствием реализации которой является физический ущерб всей системе.

Шундай таҳдидки, унинг амалга оширили-

## У

ши оқибатида бутун тизимга физик зарар етказилади.

### **Уничтожение информации**

**uz** - ахборотни йўқ қилиш

**en** - data destruction

Случайное или умышленное стирание информации на ее носителях при обработке техническими средствами, в том числе хищение носителей и технических средств.

Техник воситалар билан қайта ишлашда ташувчилардаги ахборотни тасодифан ёки қасдан ўчириш, шу жумладан, ташувчилар ва техник воситаларни ўғирлаш.

### **Управление**

**uz** - бошқариш

**en** - controlling

Процесс целенаправленного воздействия на объект, осуществляемый для организации его функционирования в соответствии с заданными требованиями.

Объектга мақсадга йўналтирилган таъсир этиш жараёни. Берилган талабларга мувофиқ унинг ишлашини ташкил қилиш учун амалга оширилади.

### **Управление безопасностью**

**uz** - хавфсизликни бошқариш

**en** - security control

Служба управления и контроля доступа к ресурсам сети. Осуществляет запуск механизмов защиты от внешних атак и проверяет целостность данных при их хранении и передаче через сеть.

Тармок ресурсларидан эркин фойдаланишни бошқариш ва назорат қилиш хизмати. Ташқи хужумлардан муҳофаза механизми ишга туширилишини амалга оширади ва маълумотларни, уларни сақлаш ва тармок орқали узатишда яхлитлигини текширади.

### **Управление доступом**

**uz** - эркин фойдаланишни бошқариш

**en** - access control

1. Методы, обеспечивающие возможность обращения к ресурсам системы обработки данных только уполномоченным логическим объектам и только разрешенным способом.

## У

2. Метод защиты информации регулированием использования всех ресурсов системы (элементов баз данных, программных и технических средств).
3. Предупреждение несанкционированного использования ресурса
4. Процесс ограничения доступа к ресурсам системы только разрешенным программам, процессам или другим системам (в сети).

1. Маълумотларни қайта ишлаш тизими ресурсларига фақат ваколатга эга мантиқий объектлар ва фақат рухсат этилган усул билан муружаат қилиш имкониятини таъминлайдиган методлар.

2. Тизимнинг барча ресурсларидан (маълумотлар базалари элементлари, дастурий ва техник воситалари) фойдаланишни тартибга солиш билан ахборотни муҳофаза қилиш методи.

3. Ресурсдан рухсат этилмаган тарзда фойдаланилишининг олдини олиш.

4. Фақат рухсат этилган дастурлар, жараёнлар ёки бошқа тизимларга (тармоқдаги) тизим ресурсларидан эркин фойдаланишни чеклаш жараёни.

### Управление доступом дискреционное

uz - эркин фойдаланишни дискрецион бошқариш

en - discretionary access control, DAC

Разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому равноправному субъекту.

Номма-ном кўрсатилган субъектлар ва номма-ном кўрсатилган объектлар ўртасидаги фойдаланишни белгилаш. Фойдаланишининг маълум ҳуқуқига эга субъект бу ҳуқуқни исталган бошқа тенг ҳуқуқли субъектга бериши мумкин.

## У

### Управление доступом избирательное

**uz** - эркин фойдаланишни таъланган бошқариш  
**en** - discretionary access control, DAC

Метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит. Управление является избирательным в том смысле, что субъект с определенными правами может осуществлять передачу прав любому объекту независимо от установленных ограничений (доступ может быть осуществлен и не напрямую).

Фойдаланувчи, жараён ваёки у тегишли бўлган гурухни идентификация қилиш ва аниқлашга асосланган, тизим субъектларнинг объектлардан фойдалана олишини бошқариш методи. Маълум ҳуқуқларга эга субъект исталган объектга белгиланган чеклашлардан қатъи назар, ҳуқуқлар беришни амалга ошира олади эркин (фойдаланиш бевосита ҳам амалга оширилиши мумкин) деган маънода бошқариш таъланган бўлади.

### Управление доступом логическое

**uz** - эркин фойдаланишни мантиқий бошқариш  
**en** - logical access control

Использование механизмов, обеспечивающих управление доступом к данным или информации. Например, использование пароля.

Маълумотлар ёки ахборотдан фойдалана олиш бошқарилишини таъминлайдиган механизмларнинг қўлланилиши. Масалан, паролнинг қўлланилиши.

### Управление доступом полномочное

**uz** - фойдаланишни ваколатли бошқариш  
**en** - mandatory ac-

Способ управления доступом к объектам, основанный на степени секретности или критичности информации (представленной специальными метками), содержащейся в объекте и формальной проверке полномочий и прав субъекта при доступе к информации данного уровня критичности.

cess control, MAC

Объектлардан эркин фойдаланишни бошқариш усули объектда мавжуд бўлган ахборотнинг (махсус белгилар билан такдим этилган) махфийлик ёки критиклик даражасига ва берилган критиклик даражасидаги ахборотдан эркин фойдаланишда субъектнинг ваколатлари ва ҳуқуқларини расман текширишга асосланган.

**Управление информационным потоком**

**uz** - ахборот оқимини бошқариш  
**en** - information flow control

1. Процедуры управления информационным потоком, удостоверяющие, что информация не может передаваться с верхних уровней безопасности на нижние (в соответствии с положениями модели Белла-Лападула).

2. Процедуры управления, удостоверяющие, что информация не может передаваться по скрытым каналам, т.е. в обход политики безопасности.

1. Ахборот хавфсизликнинг юқори даражасидан қуйи даражасига (Белла-Лападула модели қоидаларига мувофиқ) узатилиши мумкин эмаслигини тасдиқловчи ахборот оқимини бошқариш процедуралари.

2. Ахборот яширин каналлар бўйлаб, яъни хавфсизлик сиёсатини четлаб ўтиб, узатилиши мумкин эмаслигини тасдиқловчи бошқариш процедуралари.

**Управление ключами**

**uz** - калитларни бошқариш  
**en** - key management

Генерация, хранение, распределение, удаление, учет и применение ключей в соответствии с политикой безопасности.

Хавфсизлик сиёсатига мувофиқ калитларни генерациялаш, сақлаш, таксимлаш, чиқариб ташлаш, ҳисобга олиш ва қўллаш.

**Управление прикладное**

Набор функций, способствующих предоставлению пользователям возможности на-

## У

**uz** - амалий бошқариш  
**en** - application management

блюдать и управлять выполнением операций распределенной обработки данных.

Фойдаланувчиларга маълумотларни таксимланган қайта ишлаш операцияларининг бажарилишини бошқариш ва кузатиб бориш имкониятини берувчи функциялар тўплами.

### Управление рисками

**uz** - риск (этимологий хавф) ларни бошқариш  
**en** - risk management

1. Последовательность операций, выработанных практикой управления в области безопасности систем или сетей.  
2. Процесс определения контрмер в соответствии с оценкой рисков.

1. Тизимлар ёки тармоқлар хавфсизлиги соҳасида бошқариш амалиёти давомида ишлаб чиқилган операциялар кетма-кетлиги.  
2. Риск (этимологий хавф)ларни баҳолашга мувофиқ, қарши чора-тадбирларни белгилаш жараёни

### Уровень безопасности

**uz** - хавфсизлик даражаси  
**en** - security level

1. Совокупность иерархического грифа секретности и категории безопасности, которая указывает на чувствительность объекта к категории допуска лица.  
2. Комбинация иерархической классификации (уровень доступа) и неиерархической категории, представляющих уровень критичности (чувствительности) информации.

1. Объектнинг шахс фойдаланиш ҳуқуқи категориясига сезгирлигини кўрсатадиган йерархик махфийлик грифи ва хавфсизлик категорияси жами.  
2. Ахборотнинг критиклик (сезгирлик) даражасини кўрсатувчи, ноиерархик категория ва иерархик классификация (фойдалана олиш даражаси) бирикмаси.

## У

### **Уровень безопасности базовый**

**uz** - базавий хавфсизлик даражаси  
**en** - baseline security

### **Уровень доступа**

**uz** - эркин фойдаланиш даражаси  
**en** - access level

### **Уровень полномочий субъекта**

**uz** - субъект ваколатлари даражаси  
**en** - subject privilege

Обязательный минимальный уровень защищенности для информационных систем.

Муҳофаза қилинганликнинг ахборот тизимлар учун қабул қилинган, мажбурий бўлган энг паст даражаси.

1. Уровень полномочий, необходимый логическому объекту для получения доступа к защищенному ресурсу. Например, полномочия на доступ к данным или информации заданного уровня безопасности.

2. Иерархическая часть метки уровня безопасности, используемая для идентификации критичности данных или прозрачности субъектов. Уровень доступа вместе с иерархическими категориями составляет уровень безопасности.

1. Мантқиқий объектга муҳофаза қилинган ресурсдан эркин фойдаланиш имкониятини олиш учун зарур бўлган ваколат даражаси. Масалан, берилган хавфсизлик даражасидаги ахборотдан ёки маълумотлардан фойдаланиш юзасидан ваколатлар.

2. Маълумотларнинг критиклигини ёки субъектларнинг очиклигини идентификация қилиш учун қўлланиладиган, хавфсизлик даражаси белгисининг иерархик қисми. Эркин фойдаланиш даражаси ноиерархик категориялар билан бирга хавфсизлик даражасини ташкил этади.

Совокупность прав доступа субъекта доступа.

Фойдалана олиш субъектининг фойдалана олиш (кира олиш) юзасидан ҳуқуқларининг жами.



## У

### Уровень прозрачности

**uz** - очиклик даражаси

**en** - transparency level, clearance

Максимальный уровень безопасности, доступ к которому разрешен данному субъекту правилами модели Белла-Лападула. Текущий уровень субъекта (уровень, на котором он в данный момент выполняет операции) может варьировать от минимального до уровня прозрачности.

Хавфсизликнинг максимал даражаси, субъектга ундан фойдалана олиш учун Белла-Лападула модели қоидаларига кўра рухсат берилган. Субъектнинг жорий даражаси (у шу вақтда операциялар бажараётган даража) минималдан очиклик даражасигача ўзгартирилиши мумкин.

### Услуга аутентификации

**uz** - аутентификация қилиш хизмати

**en** - authentication service

Услуга, предоставляющая доказательство того, что идентификация объекта или субъекта на самом деле является идентификацией, которая заявлена им.

*Примечание: В зависимости от действующего субъекта и целей идентификации могут потребоваться следующие виды аутентификации: аутентификация пользователя, аутентификация одноранговых объектов, аутентификация источника данных.*

Объект ёки субъектни идентификациялаш аслида улар томонидан баён қилинган идентификация эканлигининг далилини кўрсатувчи хизмат.

*Изоҳ: Амалдаги субъектга ва идентификация мақсадларига боғлиқ равишда қуйидаги аутентификация турлари талаб қилиниши мумкин: фойдаланувчини аутентификация қилиш, битта ранг объектларини аутентификация қилиш, маълумотлар манбаини аутентификация қилиш.*

### Услуга безопасности

**uz** - хавфсизлик

Услуга, предоставляемая каким-либо уровнем взаимосвязи открытых систем, которая гарантирует достаточную защиту систем

## У

хизмати  
en - security service

или процессов передачи данных.

Очиқ тизимлар ўзаро боғлиқлигининг қандайдир даражаси тақдим этадиган хизмат. Маълумотлар узатиш тизимлари ёки жараёнларининг етарлича муҳофаза қилинишини кафолатлайди.

**Услуга конфиденциальности**  
uz - конфиденциаллик хизмати  
en - confidentiality service

Услуга конфиденциальности предоставляет защиту от неразрешенного раскрытия данных обмена.

*Примечание: Различают следующие виды услуг обеспечения конфиденциальности: конфиденциальность выбранного поля; конфиденциальность в режиме с установлением соединения; конфиденциальность в режиме без установления соединения; конфиденциальность трафика.*

Алмашинадиган маълумотларнинг рухсат этилмаган тарзда ошкор этилишдан муҳофаза қилинишини ифодаладиган конфиденциаллик хизмати.

*Изоҳ: Конфиденциалликни таъминлаш хизматларининг қуйидаги турлари ажратилади: танланган майдон конфиденциаллиги; боғланиш ўрнатилган режимдаги конфиденциаллик; боғланиш ўрнатилмаган режимдаги конфиденциаллик; трафикнинг конфиденциаллиги.*

**Услуга отметки времени**  
uz - вақтни белгилаш хизмати  
en - time stamping service

Услуга, которая подтверждает существование электронных данных в определенный момент времени.

*Примечание: Услуги отметки времени полезны и, возможно, совершенно необходимы для поддержки проверки цифровых подписей в течение длительного срока.*

Маълум бир вақт онда электрон маълумотлар мавжудлигини тасдиқлайдиган хизмат.

*Изоҳ: Вақтни белгилаш хизматлари фойдали, шунингдек, узоқ муддат мобайнида рақамли*

## У

*имзолар текишувини олиб бориш учун мутлақо зарур.*

### **Услуга рассылки ключей**

**uz** - калитларни тарқатиш хизмати  
**en** - key distribution service

Услуга безопасной рассылки ключей уполномоченным объектам, выполняемая центром рассылки ключей.

Калитларни ваколатли объектларга хавфсиз тарқатиш хизмати. Калитларни тарқатиш маркази томонидан бажарилади.

### **Услуга целостности**

**uz** - яхлитлик хизмати  
**en** - integrity service

Предоставление способов гарантирования правильности данных обмена, защиты от изменения, удаления, создания (вставки) и повторного использования данных обмена.

Алмашинадиган маълумотлар тўғрилигини, алмашинадиган маълумотларнинг ўзгаришлардан, чиқариб ташлашлардан, яратиш (киритиш) ва такрор фойдаланишдан муҳофаза қилинишини кафолатлаш усуллари-нинг тақдим этилиши.

### **Установление подлинности криптографическое**

**uz** - ҳақиқийликни криптографик аниқлаш  
**en** - cryptographic authentication

Установление подлинности, основанное на криптографических преобразованиях, использующих симметричное шифрование или шифрование с открытым ключом.

Симметрик шифрлаш ёки очик калит билан шифрлашдан фойдаланиладиган криптографик ўзгартиришларга асосланган ҳолда ҳақиқийликни аниқлаш.

### **Установление последовательности сообщения**

**uz** - хабарларнинг кетма-кетлигини аниқлаш  
**en** - message sequencing

Установление последовательности сообщения включает: повторное использование сообщений; изменение порядка следования сообщений; передачу сообщений ранее назначенного времени; задержку сообщений.

У хабарлардан такрор фойдаланишни; хабарлар бориш тартиби ўзгаришини; хабарлар-

нинг белгиланган вақтдан олдин узатилишини; хабарларнинг кечикишини ичига олади.

**Устойчивость**  
uz - барқарорлик  
en - robustness

Способность сети сохранять работоспособное состояние во времени и в условиях, создаваемых воздействиями внешних и внутренних дестабилизирующих факторов. Устойчивость характеризуется свойствами надежности и живучести.

Тармоқнинг ички ва ташқи барқарорлаштирувчи омиллар таъсирида вужудга келадиган шароитлар ҳамда вақтда ишчанлик ҳолатини сақлаш қобилияти. Барқарорлик ишончлилик ва яшовчанлик хусусиятлари билан тавсифланади.

**Устройство выдачи сигнала тревоги**  
uz - тревога сигналини бериш қурилмаси  
en - alert signal transmitting device

Программно-аппаратное устройство, обеспечивающее выдачу звукового и/или светового сигнала на контрольный пост в случае попыток несанкционированного доступа.

Рухсат этилмаган тарзда фойдаланишга уриниш бўлганда назорат постига товуш ва/ёки ёруғлик сигнали узатилишини таъминловчи дастурий-аппарат қурилма.

**Устройство закладное электронное специальное**  
uz - махсус (яширин) ўрнатиладиган электрон қурилма  
en - special electronic inset device

Электронное устройство, несанкционированно и замаскированно установленное в техническом средстве обработки информации, чтобы в нужный момент времени обеспечить утечку информации, нарушение ее целостности или блокирование.

Зарур вақт онида ахборотнинг чиқиб кетишини, унинг яхлитлиги бузилишини ёки блокировка қилинишини таъминлаш учун рухсатсиз ва яширин ҳолда техник воситада ўрнатилган электрон қурилма.

**Устройство защи-**

Устройство электронного или другого типа,

## У

**ты техническое**  
**uz** – техник мухофаза қурилмаси  
**en** - technical protection device

предотвращающее возможность работы с программой лицам, не имеющим такого устройства.

**Устройство защиты электронное**  
**uz** - электрон мухофаза қурилмаси  
**en** - dongle

Электрон ёки бошқа турдаги қурилма. Бундай қурилмага эга бўлмаган шахсларга дастур билан ишлаш имкониятини бермайди.

Электронное устройство в составе компьютера, выполняющее функции замка, ответчика и т.п. и предназначенное для защиты программы и данных от несанкционированного доступа.

**Устройство защиты электронное активное**  
**uz** - актив электрон мухофаза қурилмаси  
**en** - active dongle

Компьютер таркибидаги қулф, жавоб бергич ва ш.к. функцияларни бажарувчи ва дастурни ҳамда маълумотларни рухсат этилмаган тарзда фойдаланишдан мухофаза қилиш учун мўлжалланган электрон қурилма.

Электронное устройство защиты, выполненное на основе заказной микросхемы, имеющее электрически программируемую энергонезависимую память и присоединяющееся к параллельному порту.

**Устройство кодирующее**  
**uz** - кодловчи қурилма  
**en** - coder

Буюртма микросхема асосида ясалган, электр дастурлаштириладиган энергияга боғлиқ бўлмаган хотирага эга ва параллел портга уланадиган электрон мухофаза қурилмаси.

1. Автоматическое или автоматизированное устройство для кодирования программ и данных на носителе информации с целью последующего их ввода в ЭВМ.

2. Устройство для преобразования вида представления информации, в котором каждому входному сигналу соответствует определен-

ная комбинация выходных сигналов, являющихся кодом входного сигнала.

1. Дастурлар ва маълумотларни ахборот ташувчисигади уларни кейинчалик ЭХМга киритиш мақсадида кодлаш учун мўлжалланган автоматик ёки автоматлаштирилган қурилма.

2. Ахборотни тақдим этиш шаклини ўзгартирувчи қурилма, бунда ҳар бир кириш сигнаliga кириш сигнаlining коди ҳисобланадиган чиқиш сигналларининг маълум комбинацияси мос келади.

**Устройство многоуровневое**

**uz** - кўп даражали қурилма

**en** - multilevel device

Функциональный блок, который может одновременно обрабатывать данные двух или более уровней безопасности без риска нарушения компьютерной безопасности.

Компьютер хавфсизлигининг бузилиш rischi (эхтимолий хавфи) бўлмаган ҳолда икки ёки ундан кўп хавфсизлик даражасигади маълумотларни бир вақтнинг ўзида қайта ишлай олиши мумкин бўлган функционал блок.

**Устройство одноуровневое**

**uz** - бир даражали қурилма

**en** - single-level device

Функциональный блок, который может обрабатывать в данное время данные только одного уровня безопасности.

Берилган вақтда битта хавфсизлик даражасигади маълумотларни қайта ишлай олиши мумкин бўлган функционал блок.

**Устройство повышения достоверности идентификации**

**uz** - идентификациялаш ишончили-

Программно-аппаратное устройство, обеспечивающее корректировку ошибок идентификации, переданных с удаленных терминалов по каналам телекоммуникаций.

*Примечание: Для корректировки ошибок используются различные способы: обратная посылка сообщений на передающий конец для сравнения*

## У

лигини ошириш  
қурилмаси  
**en** - identification  
integrity increase  
device

*его с оригиналом; посылка одновременно с сообщением контрольных разрядов; использование избыточных кодов (код Хемминга, циклические коды) и т.д.*

Телекоммуникациялар каналлари орқали олисдаги терминаллардан узатилган идентификация хатолари тузатилишини таъминлайдиган дастурий-аппарат қурилма.

*Изоҳ: Хатоларни тузатиш учун турли усуллар; хабарларни узатувчи томонга оригинал билан таққослаш учун қайта юбориш; хабар билан бир вақтда назорат разрядларини юбориш; ортиқча кодлардан (Хемминг коди, циклик кодлар) фойдаланиш ва ҳ.к. қўлланилади.*

Устройство прерывания программы пользователя

**uz** - фойдаланувчи дастурини тўхтатиб қўйиш қурилмаси  
**en** - user program interrupt device

Программно-аппаратное устройство, обеспечивающее прерывание (блокирование) программы пользователя в случае попыток несанкционированного доступа.

Рухсат этилмаган тарзда фойдаланишга уриниш бўлганда, фойдаланувчи дастурининг тўхтатиб қўйилишини (блокировка қилинишини) таъминлайдиган дастурий-аппарат қурилма.

Устройство регистрации доступа пользователей

**uz** - фойдаланувчиларнинг эркин фойдаланишини қайд этиш қурилмаси  
**en** - users access registration device

Программно-аппаратное устройство, обеспечивающее регистрацию пользователей при всех их обращениях к системе с указанием номера терминала, даты и времени обращения.

Тизимга қилинган барча муурожаатлар пайтида, терминал рақамини, муурожаат санаси ҳамда вақтини кўрсатган ҳолда фойдаланувчиларнинг қайд этилишини таъминлайдиган дастурий-аппарат қурилма.

Устройство стирания данных

Программно-аппаратное устройство, обеспечивающее стирание оставшихся после

## У

**uz** - маълумотларни ўчириш қурилмаси  
**en** - data cancellation device

обработки данных в ОЗУ путем записи нулей во все ячейки соответствующего блока памяти.

Оператив-хотира қурилмасида қайта иш-лашдан кейин қолган маълумотларнинг, тегишли хотира блокининг барча ячейка-рига ноллар ёзиш йўли билан ўчирилишини таъминлайдиган дастурий-аппарат қурилма.

### Устройство элек-тромагнитного зашумления

**uz** - электромагнит шовқин қурилмаси  
**en** - electromagnetic noise masking

Широкополосный излучатель (генератор) электромагнитного шума, предназначенный для маскировки (подавления) информационного электромагнитного поля, создаваемого техническими средствами обработки информации, или наводок в токопроводящих коммуникациях в заданной полосе частот.

Белгиланган частоталар полосасида, ахборотни қайта ишлаш техник воситалари вужудга келтирадиган информацион электромагнит майдонни никоблаш (бостириш) ёки ток ўтказадиган коммуникацияларда тўғри-лашлар учун мўлжалланган кенг полосали, электромагнит шовқин нурлатгич (генератори).

### Утечка информа-ции

**uz** - ахборотнинг чиқиб кетиши (йўқолиши)  
**en** - information loss

Утрата информацией при ее обработке техническими средствами свойства секретности (конфиденциальности) в результате несанкционированного ознакомления с нею или несанкционированного документирования (снятия копий).

Ахборотни техник воситалар билан қайта ишлашда, рухсат этилмаган тарзда танишиш ёки ҳужжатлаштириш (нусха олиш) натижасида ахборотнинг махфийлик (конфиденциаллик) хусусиятини йўқолиши.



**Утечка секретной информации**

**uz** - махфий ахборотнинг чиқиб кетиши (йўқолиши)  
**en** - secret information leaking

Неправомерное распространение сведений, составляющих государственную и служебную тайну, за пределы организации или круга лиц, которым эти сведения доверены (обладают).

Давлат ва хизмат сири ҳисобланадиган маълумотларнинг шу маълумотлар ишониб топширилган (бундай маълумотлар бўлган) ташкилот ёки шахслар доирасидан ташқарига ноқонуний тарқатилиши.

**Утилиты скрытого администрирования**

**uz** - яширин бошқариш утилиталари  
**en** - latent administration utilities

Программы для осуществления несанкционированного администрирования удаленных компьютеров: приема/отсылки файлов, их запуска или уничтожения, вывода сообщений, удаления информации, перезагрузки компьютера и т.д.

Олисдаги компьютерларнинг рухсат этилмаган тарзда бошқарилишини амалга ошириш, яъни файлларни қабул қилиш/жўнатиш, уларни ишга тушириш ёки йўқ қилиш, хабарларни чиқариш, ахборотни ўчириш, компьютерни қайта юклаш ва ҳ.к. учун мўлжалланган дастурлар.

**Утрата секретных документов или изделий**

**uz** - махфий ҳужжатлар ёки буюмларни йўқотиш  
**en** - secret documents or articles loss

Потеря (в том числе временная) документа или изделия лицом, ответственным за их сохранность, являющаяся результатом нарушения установленных правил обращения с ними, вследствие чего эти документы или изделия стали либо могли стать достоянием посторонних лиц.

Ҳужжат ёки буюмнинг уларнинг сақланиши учун жавобгар шахс томонидан йўқотилиши (шу жумладан, вақтинчалик), бу улар билан ишлашнинг белгиланган қоидаларининг бузилиши натижаси бўлиб, оқибатда

## У

### Учет индивиду- альный

**uz** - индивидуал  
ҳисобга олиш  
**en** - individual  
accountability

бу ҳужжатлар ёки буюмлар бегона шахс-ларнинг мулкига айланади ёки айланиши мумкин.

Комплекс мер, за счет которых идентификация пользователя может быть использована для определения возможности доступа пользователя к машинам, материалам и т.п.; правила предоставления пользователю времени, методов и режимов доступа.

Фойдаланувчини идентификация қилишдан унинг машиналар, материаллар ва ш.к. дан фойдалана олиш имкониятини аниқлашда қўлланилиши мумкин бўлган чора-тадбирлар комплекси; фойдаланувчига фойдалана олиш вақти, методлари ва режимларини тақдим этиш қоидалари.

### Ущерб uz - зарар en - loss

Явное повреждение какого-либо из компонентов системы или приведение компонентов системы в неработоспособное состояние, а также различного рода утечки информации и изменение некоторых физических и логических характеристик системы.

Тизим компонентларидан бирининг очик шикастланиши ёки тизим компонентларининг ишлаш қобилияти йўқолган ҳолатга тушиб қолиши, шунингдек, ахборотнинг турли кўринишда чиқиб кетиши ҳамда тизим баъзи физик ва мантиқий характери-стикаларининг ўзгариши.

### Уязвимость uz - заифлик en - vulnerability

1. Уязвимое место или брешь в системе обработки данных.

*Примечание: Если при наличии уязвимости имеется соответствующая угроза, то существует и риск.*

2. Слабость в системных средствах защиты, вызванная ошибками или слабостями в

## У

процедурах, проекте, реализации, внутреннем контроле системы, которая может быть использована для нарушения политики безопасности системы.

3. Ошибка при назначении полномочий или упущение при разработке, реализации или управлении средствами защиты системы, которые могут привести к преодолению защиты.

4. Слабое место в защите системы, через которое можно несанкционированно проникнуть в сеть.

5. Свойство системы, которое может привести к нарушению ее защиты при наличии угрозы. Уязвимость может возникать случайно из-за неадекватного проектирования или неполной отладки или может быть результатом злого умысла.

6. Любое слабое место, которое может быть использовано для нарушения безопасности системы или информации, которая в ней содержится.

1. Маълумотларни қайта ишлаш тизимидаги заиф жой ёки камчилик.

*Изоҳ: Заифлик мавжуд бўлганда унга тегишли таҳдид, яъни риск (этимологий хавф) ҳам мавжуд бўлади.*

2. Тизим хавфсизлик сиёсатини бузиш учун қўлланилиши мумкин бўлган процедуралар, лойиҳадаги, амалга оширишдаги, тизимни ички назорат қилишдаги хатолар ёки камчиликлар келтириб чиқарган, тизим муҳофаза воситаларидаги камчилик.

3. Муҳофазани енгиб ўтишга олиб келиши мумкин бўлган, тизимнинг муҳофаза воситаларини ишлаб чиқиш, амалга ошириш ёки бошқаришдаги йўқотишлар ёки ваколатларни тайинлашдаги хато.

4. Тизимни муҳофаза қилишдаги тармоққа

## У

рухсат этилмаган тарзда сукулиб кириш мумкин бўлган заиф жой.

5. Тизимнинг таҳдид юзага келганда муҳофаза қилиниши бузилишига олиб келадиган хусусияти. Заифлик мос даражада лойиҳаланмаслик ёки тўла созланмаслик туфайли тасодифан юзага келиши ёки ёмон ният натижаси бўлиши мумкин.

6. Хавфсизлик тизимини ёки унда бўлган ахборотни бузиб кўрсатиш учун фойдаланиладиган ҳар қандай заиф жой.

### **Уязвимость автоматизированной системы**

**uz** - автоматлаштирилган тизимнинг заифлиги  
**en** - automated system vulnerability

Любая характеристика автоматизированной системы, использование которой нарушителем может привести к реализации угрозы.

Автоматлаштирилган тизимнинг бузгунчининг ундан фойдаланиши таҳдидни амалга оширишга олиб келиши мумкин бўлган ҳар қандай характеристикаси.

### **Уязвимость информации**

**uz** - ахборотнинг заифлиги  
**en** - information vulnerability

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

Ахборотнинг унинг конфиденциаллиги, яхлитлиги, ундан эркин фойдаланиш мумкинлиги бузилишига ва ноқонуний тарзда кўпайтирилишига олиб келиши мумкин бўлган турли беқарорлаштирувчи омиллар таъсирига мойиллиги.

### **Уязвимость субъекта информационных отношений**

**uz** - ахборот муносабатлари субъек-

Потенциальная подверженность субъекта нанесению ущерба его жизненно важным интересам посредством воздействия на критичную для него информацию, ее носители и процессы ее обработки.

## У

тининг заифлиги

**en** - vulnerability of information relapse

Субъектнинг унинг учун критик бўлган ахборотга, уни ташувчиларга ва қайта ишлаш жараёнларига таъсир этиш воситасида, ҳаётий муҳим манфаатларига зарар етказишига потенциал йўлиқишлиги.

## Ф

**Файл архивный**

**uz** - архивга оид файл  
**en** - archive file

Файл, сохраняемый для более позднего изучения или верификации, для безопасности или любой другой цели.

Кейинрок ўрганиш ёки верификация (асл нусха) учун, хавфсизлик ёки исталган бошқа мақсад учун сақланадиган файл.

**Файл заархивированный**

**uz** - архивлаштирилган файл  
**en** - archived file

Файл, для которого существует архивный файл.

Архивланган файли мавжуд бўлган файл.

**Файл защищенный**

**uz** - муҳофаза қилинган файл  
**en** - protected file

Файл, для доступа к записям которого необходимо ввести пароль.

Ёзувларидан фойдалана олиш учун пароль киритилиши зарур бўлган файл.

**Файл контрольной проверки**

**uz** - назорат текширув файли  
**en** - checking file

Файл, созданный оператором с целью подготовки данных для проверки.

Оператор томонидан маълумотларни текшириш учун тайёрлаш мақсадида яратилган файл.

**Файл неотображаемый**

**uz** - акс этирилмайдиган файл  
**en** - invisible file

Дисковый файл, который не указывается в справочнике диска на экране дисплея.

Дисплей экранисидаги диск справочнигида кўрсатилмайдиган диск файли.

## Ф

### **Файл резервный**

**uz** - резерв файл

**en** - backup file

Файл, создаваемый для возможно более поздней реставрации данных. Например, копия файла, сохраняемая в резервном пункте обработки данных.

Маълумотларни мумкин қадар кейинроқ тиклаш учун яратилган файл. Масалан, маълумотларни қайта ишлаш резерв пунктида сақланадиган файл нусхаси.

### **Фактор воздействующий внешний**

**uz** - таъсир этувчи

ташки омил

**en** - external

influencing factor

Внешнее воздействие на информацию или ее носитель, приводящее к искажению, уничтожению или блокированию защищаемой информации.

Муҳофаза қилинадиган ахборотнинг бузиб кўрсатилишига, йўқ қилинишига ёки блокировкаганишига олиб келувчи, ахборотга ёки уни ташувчига кўрсатиладиган ташқи таъсир.

### **Фактор дестабилизирующий**

**uz** - беқарорлашти-  
рувчи омил

**en** - destabilizing

factor

Явление или событие, нарушившее конфиденциальность, целостность и/или доступность информационных ресурсов, нарушение работоспособности сети или ее элементов. Например, угроза информационной безопасности.

Юз бериши оқибатида ахборот ресурсларининг конфиденциаллиги, яхлитлиги ва ёки улардан эркин фойдаланиш, тармоқ ёки тармоқ элементлари иш қобилиятлари бузилиши мумкин бўлган воқеа ёки ходиса. Масалан, ахборот хавфсизлигига таҳдид.

### **Фактор опасности**

**uz** - хавф омили

**en** - treat factor

Причина, обуславливающая появление угроз для безопасности информации при ее обработке техническими средствами.

*Примечание: Основными факторами опасности для информации, обрабатываемой тех-*

## Ф

*ническими средствами, являются: побочные электромагнитные излучения и наводки; несанкционированный доступ к информации штатными техническими средствами; специальные электронные закладные устройства (аппаратные закладки); внешние воздействия на информационный ресурс.*

Ахборотни техник воситалар билан қайта ишлашда унинг хавфсизлиги учун тахдидлар пайдо бўлишини шартловчи сабаб.

*Изоҳ: Ёндош электромагнит нурланишлар ва тўғрилашлар, ахборотдан штат техник воситалари билан рухсат этилмаган тарзда фойдаланиш, махсус электрон ўрнатувчи қурilmалар; ахборот ресурсига бўладиган ташиқи таъсирлар техник воситалар билан қайта ишланадиган ахборот учун асосий хавф омиллари ҳисобланади.*

### **Фальсификация**

**uz** - сохталаштириш  
**en** - falsification

Использование различных технологий для обхода систем управления доступом на основе IP-адресов с помощью маскирования под другую систему, применяя ее IP-адрес.

Бошқа тизим остида ниқобланиш ёрдамида, унинг IP адресидан фойдаланиб, IP адреслар асосида эркин фойдаланишни бошқариш тизимларини четлаб ўтиш учун турли технологиялардан фойдаланиш.

### **Фиксация авторства**

**uz** - муаллифликни қайд этиш  
**en** - non-repudiation

1. Способность предотвратить последующее непризнание отправителем факта отправки сообщения или выполнения действия.
2. Защита от отказа признания одним из участвующих в сеансе связи объектов участия во всем или в части сеанса связи.
3. Процесс, обеспечивающий невозмож-

## Ф

ность непризнания отправителем сообщения (например, запроса на услугу "разовая плата за просмотр программы") факта его направления.

1. Жўнатувчининг хабарни жўнатиш ёки ҳаракатни бажариш фактини кейинчалик тан олмаслигини бартараф қилиш қобилияти.
2. Объектларни алоқа сеансида иштирок этувчилардан бири томонидан, алоқа сеансининг барчасида ёки бир қисмида иштирок этганликни тан олишни рад этишдан муҳофаза қилиш.
3. Жўнатувчи томонидан хабарни (масалан, «дастурни кўриш учун бир марталик тўлов» хизматига сўров), унинг жўнатиш фактини тан олмаслик мумкин эмаслигини таъминловчи жараён.

### **Фиксация контроля средств защиты**

**uz** - муҳофаза воситалари назорат

қилинишини қайд

этиш

**en** - security audit trail

Совокупность сведений о состоянии средств защиты, накапливаемых во времени и предназначенных для упрощения управления средствами защиты.

Вақт бўйича тўпланадиган ва муҳофаза воситаларини бошқаришни соддалаштириш учун мўлжалланган, муҳофаза воситаларининг ҳолати тўғрисидаги маълумотлар жами.

### **Философия защиты**

**uz** - муҳофаза фалсафаси

**en** - protection

philosophy

Общая схема системы в целом, позволяющая видеть использование механизмов защиты (формальными и неформальными методами).

Муҳофаза механизмларидан фойдаланишни (расмий ёки норасмий методлар билан) кўришга имкон берувчи, тизимнинг тўла умумий схемаси.



## Ф

### **Фильтр безопасности**

**uz** - хавфсизлик  
фильтри  
**en** - security filter

Доверенная компьютерная система, которая реализует политику безопасности для данных, циркулирующих в системе.

Тизимда айланувчи маълумотларнинг хавфсизлик сиёсатини амалга оширадиган ишончли компьютер тизими.

### **Фильтрация входящего трафика**

**uz** - кирувчи трафик-  
ни филтрлаш  
**en** - ingress filtering

Сортировка входящего трафика маршрутизатора с отбрасыванием пакетов, адреса отправителей которых не используются в общем сетевом адресном пространстве.

Жўнатувчиларнинг адресларидан умумий тармоқ адрес майдонида фойдаланилмайдиган пакетларни ташлаб юбориш билан маршрутизаторнинг кирувчи трафигини саралаш.

### **Фильтрация исходящего трафика**

**uz** - чикувчи трафик-  
ни филтрлаш  
**en** - egress filtering

Сортировка исходящего трафика маршрутизатора с отбрасыванием пакетов, адреса отправителей которых не включены в диапазон адресов, используемых во внутренней сети.

Жўнатувчиларнинг адреслари ички тармоқда фойдаланиладиган адреслар диапазонида киритилмаган пакетларни ташлаб юбориш билан маршрутизаторнинг чикувчи трафигини саралаш.

### **Флаг**

**uz** - байрок  
**en** - flag

Часть формата элемента данных из одного или нескольких битов, которые определяют статус этого элемента.

Бир ёки бир неча битдан иборат маълумотлар элементи форматининг бир қисми. Битлар бу элементнинг статусини белгилайди.

## Ф

### **Формат диска**

**uz** - диск формати

**en** - disk format

Способ размещения информации на гибком диске, обеспечивающий идентификацию, контроль и верификацию данных.

Ахборотни эгилувчан (юмшок) дискда жойлаштириш усули. Маълумотларнинг идентификация, назорат ва верификация қилинишини таъминлайди.

### **Фрод внутренний**

**uz** - ички фрод

**en** - internal fraud

Вид криминальной деятельности, когда служащие используют свое служебное положение для получения выгоды лично или через третьих лиц путем передачи им сведений конфиденциального характера.

Жиноий фаолият тури бўлиб, хизматчилар ўзларининг хизмат мавқеларидан шахсан ёки учинчи шахслар орқали, уларга конфиденциал характердаги маълумотларни бериш йўли билан манфаат кўришда фойдаланадилар.

### **Фрод, основанный на услуге переадресации вызова**

**uz** - чакирувни қайта

йўллаш хизматиға

асосланган фрод

**en** - premium rate service fraud, PRS fraud

Метод получения якобы «легального» дохода, основанный на переадресации дорогостоящих вызовов на собственные каналы, как правило, развернутые в других странах.

Гўёки, «конуний» даромад олиш методи бўлиб, одатда, бошқа мамлакатларда ташкил этилган ўз каналларига киммат чакирувларни қайта йўллашга асосланган.

### **Фрод хакерский**

**uz** - хакерлик фроди

**en** - hacking fraud

Вид мошенничества, связанный со взломом защиты сети и получением несанкционированного доступа к сетевым ресурсам.

Тармоқ муҳофазасини бузиш ва тармоқ

## Ф

ресурсларидан рухсат этилмаган тарзда фойдаланиш билан боғлиқ фирибгарлик тури.

**Фродастер**  
uz - фродастер  
en - fraudster

Лицо, пользующееся услугами мобильной связи без их оплаты или получающее какие-либо иные выгоды.

Мобил алоқа хизматларидан уларнинг ҳақини тўламадан фойдаланувчи ёки қандайдир бошқача фойда оладиган шахс.

**Функция односторонняя**  
uz - бир томонлама функция  
en - one-sided function

Функция, для которой по заданному аргументу  $x$  легко вычислить значение функции  $f(x)$ , тогда как определение  $x$  из  $f(x)$  трудно вычислимо. До сих пор строго не доказано, что односторонние функции существуют. Для шифрования информации односторонние функции не применимы, так как расшифровать текст, зашифрованный с их помощью, не сможет даже законный владелец. В криптографии используются однонаправленные функции с секретом.

Берилган  $x$  аргумент бўйича  $f(x)$  функция қиймати осон ҳисоблаб чиқариладиган функция.  $f(x)$  ни  $x$  дан ҳисоблаб чиқариш анчагина мураккаб. Ҳозиргача бир томонлама функцияларнинг мавжудлиги қатъий исботланмаган. Ахборотни шифрлаш учун бир томонлама функцияларни қўллаб бўлмайди, чунки улар ёрдамида шифрланган матнни ҳатто унинг қонуний эгаси ҳам расшифровка қила олмайди. Криптографияда сири бўлган бир томонлама функциядан фойдаланилади.

## Ф

### Функция односторонняя с секретом

**uz** - сирин бўлган бир томонлама функция  
**en** - one-sided secret function

Функция  $f_k(x)$ , зависящая от параметра  $k$  такая, что при известном  $k$  можно найти полиномиальные алгоритмы  $E_k$  и  $D_k$ , позволяющие легко вычислить  $f_k(x)$  для всех  $x$  и  $f_k^{-1}(y)$  для всех  $y$ , а нахождение  $f_k^{-1}(y)$  без знания  $k$  трудно вычислимо (полиномиального алгоритма не существует) даже при известном алгоритме  $E_k$ . На основе понятия односторонней функции с секретом был предложен принцип открытого распределения ключей и, как следствие, криптосистемы с открытым ключом.

$k$  параметрга боғлиқ бўлган  $f(x)$  функция, бу шундай функцияки,  $k$  маълум бўлганда, барча  $x$  лар учун  $f_k(x)$  ни, барча  $y$  лар учун  $f_k^{-1}(y)$  ни осон ҳисоблаб чиқариш имконини берадиган  $E_k$  ва  $D_k$  полиномиал алгоритмларни топиш мумкин.  $k$  ни билмасдан туриб,  $f_k^{-1}(y)$  ни топиш, ҳатто  $E_k$  алгоритм маълум бўлганда ҳам, ҳисоблаб чиқариш мураккаб бўлган вазифа (полиномиал алгоритм мавжуд эмас). Сирин бўлган бир томонлама функция тушунчаси асосида калитларни очиқ таксимлаш, унинг натижасида очиқ калитли криптотизим принципи таклиф қилинган.

### Функция шифрования

**uz** - шифрлаш функцияси  
**en** - encryption function

Функция, используемая в шифре для преобразования данных с применением ключа.

Шифрда маълумотларни калит қўлланилган ҳолда ўзгартириш учун фойдаланиладиган функция.

## Х

**Хост-бастион**  
**uz** - хост-бастион  
**en** - bastion host

Компьютер-шлюз, на котором работает программное обеспечение межсетевого экрана и который устанавливается между внутренней и внешней сетями. К хост-бастионам можно отнести шлюзы сеансового и прикладного уровней, а также межсетевые экраны, использующие технологию Stateful inspection.

Тармоқлараро экраннинг дастурий таъминоти ишлайдиган ва ички ҳамда ташқи тармоқлар ўртасида ўрнатиладиган компьютер-шлюз. Хост-бастионларга сеанс ва амалий даражадаги шлюзларни, шунингдек, Stateful inspection технологиясидан фойдаланувчи тармоқлараро экранларни киритиш мумкин.

**Хэш**  
**uz** - хэш  
**en** - hash

Блок данных фиксированного размера, полученный в результате хэширования массива данных.

Маълумотлар массивини хэшлаш натижасида олинган, қатъий ўлчамдаги маълумотлар блоқи.

**Хэш-алгоритм защищенный**  
**uz** - муҳофазаланган хэш-алгоритм  
**en** - secure hash algorithm

Хэш-алгоритм, позволяющий генерировать электронные подписи.

Электрон имзоларни генерациялаш имконини берадиган хэш-алгоритм.

**Хэширование**  
**uz** - хэшлаш  
**en** - hashing

1. Процесс вычисления значения хэш-функции.  
2. Преобразования массива данных произвольного размера в блок данных фиксированного размера, служащий заменителем исходного массива в некоторых контекстах.

## Х

1. Хэш-функция қийматларини ҳисоблаш жараёни.
2. Баъзи бир матн бўлақларида дастлабки массивнинг ўрнини босишга хизмат қилувчи ихтиёрий ўлчамдаги маълумотлар массивини белгиланган ўлчамдаги маълумотлар блокига алмаштириш.

**Хэш-функция**  
(**функция хэширования**)

**uz** - хэш-функция  
(хэшлаш функцияси)  
**en** - hash-function

1. Функция, отображающая строку бит в строку бит фиксированной длины.
2. Математическое преобразование массива данных произвольного размера и вычисление для него фиксированной уникальной последовательности небольшой длины.

1. Битлар сатрини белгиланган узунликдаги битлар сатрига айлантириш функцияси.
2. Ихтиёрий ўлчамдаги маълумотлар массивини математик алмаштириш ва унинг учун унча узун бўлмаган белгиланган ягона кетма-кетликни ҳисоблаш.

## Ц

**Целостность**  
**uz** - яхлитлик  
**en** - integrity

Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Ахборотнинг бузилмаган кўринишда (ахборотнинг қандайдир қайд этилган ҳолатига нисбатан ўзгармаган шаклда) мавжуд бўлишида ифодаланадиган хусусияти.

**Целостность данных**  
**uz** - маълумотларнинг яхлитлиги  
**en** - data integrity

1. Способность данных сохранять точность и непротиворечивость независимо от вынимаемых изменений.
2. Свойство, гарантирующее невозможность изменения, подмены или уничтожения данных несанкционированным способом.

*Примечание: Целостность данных включает*

## Ц

*устойчивость системы к отказам и автоматическое восстановление.*

1. Амалга ошириладиган ўзгартиришлардан қатъи назар, маълумотларнинг аниқликни ва зид келмасликни сақлаш қобилияти.
2. Маълумотларни рухсат этилмаган усулда ўзгартириб, ўрнини алмаштириб ёки йўқ қилиш мумкин бўлмаслигини кафолатлайдиган хусусият.

*Изоҳ: Маълумотларнинг яхлитлиги тизимнинг бузилишларга чидамлилигини ва автоматик тикланишини ичига олади.*

### **Целостность информации**

**uz** - ахборотнинг яхлитлиги  
**en** - information integrity

Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Ҳисоблаш техникаси воситалари ва автоматлаштирилган тизимнинг тасодифий ва ёки қасдан бузиб кўрсатиш (бузиш) шароитида ахборотнинг ўзгармаслигини таъминлаш хусусияти.

### **Целостность системы**

**uz** - тизимнинг яхлитлиги  
**en** - system integrity

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.

Маълумотларни қайта ишлаш тизимининг, ўзининг оператив вазифасини бажариш билан бир вақтда, рўйхатга олинмаган фойдаланувчилар томонидан ресурслардан фойдаланишнинг ёки ўзгартирилишининг олдини олиш, шунингдек, рўйхатга олинган

## Ц

фойдаланувчилар томонидан уларга тегишли бўлмаган ресурслардан фойдаланишнинг ёки ўзгартирилишининг олдини олиш хусусияти.

### **Цель защиты информации**

**uz** - ахборотни муҳофаза қилиш мақсади

**en** - Information security target

Заранее намеченный уровень защищенности информации, получаемый в результате реализации системы защиты на объекте.

*Примечание: Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.*

Объектда муҳофаза қилиш тизимини амалга ошириш натижасида олинadиган ахборот муҳофаза қилинганлигининг олдиндан белгиланган даражаси.

*Изоҳ: Ахборотни муҳофаза қилишдан мақсад ахборотнинг эҳтимол тutilган тарқалиб кетиши ва/ ёки ахборотга рухсат этилмаган, кўзда тutilмаган таъсир натижасида ахборот мулкдорига, эгасига, фойдаланувчисига етказилadиган зарарнинг олдини олиш бўлиши мумкин.*

### **Центр аутентификации**

**uz** - аутентификация қилиш маркази

**en** - authentication center, AuC

Сетевое оборудование, отвечающее за конфиденциальный обмен информацией в сети мобильной связи и обеспечивающее защиту от несанкционированного доступа.

Мобил алоқа тармоғида конфиденциал ахборот алмашиниш юзасидан жавобгар бўлган ва рухсат этилмаган тарзда фойдалана олишдан муҳофаза қилинишни таъминлайдиган тармоқ ускунаси.

### **Центр распределения ключей**

**uz** - калитларни тақсимлаш маркази

**en** - key distribution

Механизм, позволяющий распределять секретные ключи в симметричных криптосистемах.

Симметрик криптоцизмларда махфий ка-



## Ц

center литларни тақсимлаш имконини берадиган механизм.

### **Центр сертификации ключей**

uz - калитларни сертификатлаш маркази

en - key certification center

Механизм, который не требует при каждом запросе на установление защищенного соединения обращаться за ключом абонента-респондента.

Мухофазаланган боғлинишга бўлган ҳар бир сўровда абонент-респондент калитига мувожаат қилинишини талаб этмайдиган механизм.

### **Цикл ключей жизненный**

uz - калитларнинг ҳаётий цикли

en - key lifecycle

Последовательность стадий, которые проходят ключи от момента генерации до момента уничтожения.

Калитлар генерация вақтидан йўқ қилиш вақтигача ўтадиган босқичлар кетма-кетлиги.

### **Цикл проверки**

uz - текширув цикли

en - loop check

Проверка, выполняемая для определения правильности передачи данных, при которой полученные данные возвращаются к источнику для сравнения с первоначально переданными данными

Маълумотлар узатилишининг тўғрилигини аниқлаш мақсадида бажариладиган текширув. Бунда олинган маълумотлар дастлаб узатилган маълумотлар билан таққослаш учун манбага қайтарилади.

### **Цифра контрольная**

uz - назорат рақами

en - check digit

Ключ проверки, состоящий из одиночной цифры (символа).

Битта рақам (символ)дан иборат бўлган текширув калити.

## Ч

**«Черви» файловые**  
**uz - файл «куртлари»**  
**en - file worms**

Эти вирусы создают собственные копии с привлекательными для пользователя названиями (например, Game.exe, install.exe и др.) в надежде на то, что пользователь их запустит.

Фойдаланувчи ишга тушириб юборди деган умидда, унинг эътиборини тортадиган номлар остида (масалан, Game.exe, install.exe ва бошқалар) ўзининг нусхаларини яратадиган вируслар.

**«Червь»**  
**uz - «курт»**  
**en - worm**

1. Независимая программа, способная самостоятельно распространяться в системах обработки данных или компьютерных сетях.
2. Программа, распространяющаяся по сети и использующая уязвимости сетевых протоколов или сетевых программ для распространения своих копий по узлам сети, где она может быть активизирована.
3. Вредоносная программа, распространяющаяся по сети, не оставляя своей копии на магнитном носителе, вычисляющая адреса сетевых компьютеров и записывающая по этим адресам свои копии.

*Примечание: Обычно «червь» прерывает ход обработки информации в системе, оставаясь не обнаруженным, а затем самоуничтожается.*

1. Маълумотларни қайта ишлаш тизимларида ёки компьютер тармоқларида ўз ўзидан тарқалиш қобилиятига эга бўлган мустикал дастур.
2. Тармоқ бўйлаб тарқаладиган, ўзининг нусхаларини тармоқ узеллари орқали тарқатиш учун тармоқ протоколлари ёки дастурларининг заиф томонларидан фойдаланадиган дастур.
3. Ўзининг нусхаларини магнит ташувчида қолдирмаган ҳолда тармоқ бўйлаб

## Ч

таркаладиган, тармоқ компьютерларининг адресларини ҳисоблаб чиқадиган ва бу адреслар бўйича ўз нусхаларини ёзадиган зарарли дастур.

*Изоҳ:* Одатда, «курт» топиб бўлмайдиган ҳолатда қолиб, тизимда ахборотни қайта ишлаш жараёнини тўхтатиб қўяди, сўнг ўзини ўзи йўқ қилади.

**Число начальное**  
**uz** - бошланғич сон  
**en** - seed

Случайная числовая последовательность, используемая для генерации другой, обычно более длинной псевдослучайной последовательности.

Бошқа бир, янада узунроқ бўлган псевдотасодифий кетма-кетликни генерациялаш учун фойдаланиладиган тасодифий сонли кетма-кетлик.

**Число случайное**  
**uz** - тасодифий сон  
**en** - random challenge,  
**RAND**

Код, формируемый с помощью генератора псевдослучайных чисел и используемый при аутентификации, шифровании и проверке целостности.

Псевдотасодифий сонлар генератори ёрдамида шаклланиладиган ва аутентификация қилишда, шифрлашда, яхлитликни текширишда фойдаланиладиган код.

**Чтение с линии телекоммуникаций активное**  
**uz** - телекоммуникациялар линиясидан актив ўқиш  
**en** - active line-tap

Нежелательное взаимодействие с системой телекоммуникаций, при котором сигналы, данные или сообщения, передаваемые по линиям телекоммуникаций, могут быть задержаны или удалены из системы.

Телекоммуникациялар тизими билан номақбул ўзаро ҳамкорлик, бунда телекоммуникациялар линиялари орқали узилашадиган сигналлар, маълумотлар ёки хабарлар ушланиб қолиши ёки тизимдан чиқариб юборилиши мумкин.

## Ч

**Чтение с линии телекоммуникаций пассивное**

**uz** - телекоммуникациялар линиясидан пассив ўқиш

**en** - passive line-tap

**Чувствительность**

**uz** - таъсирчанлик

**en** - sensitivity

Несанкционированное чтение сигналов, данных или сообщений из системы телекоммуникаций без изменения ее сигналов.

Телекоммуникациялар тизимидан чиқадиган сигналлар, маълумотлар ёки хабарларни, тизим сигналларини ўзгартирмасдан, рухсат этилмаган тарзда ўқиш.

1. Степень важности информации, определяемая ее владельцем и указывающая на необходимость ее защиты.

2. Характеристика ресурса сети, определяющая его степень важности и, возможно, включающая уязвимость.

1. Ахборотнинг, унинг эгаси томонидан белгиланадиган ва ахборот муҳофаза қилиниши зарурлигини кўрсатадиган муҳимлик даражаси.

2. Тармоқ ресурсининг характеристикаси бўлиб, унинг муҳимлик даражасини белгилайди. Тармоқнинг заиф томонларини ҳам ичига олиши мумкин.

## Ш

**Шарада Меркля**

**uz** - Меркл шарада-си

**en** - Merkle charade

Алгоритм распределения ключей, который применяется для передачи используемого для шифрования секретного ключа, скрывая его в большом наборе шарад (головоломок).

Калитларни тақсимлаш алгоритми. Шифрлаш учун фойдаланиладиган махфий калитни, шарадаларнинг катта тўпламида уни яширган ҳолда, узатишда қўлланилади.

**Шифр**

**uz** - шифр

**en** - cipher, cypher

Совокупность обратимых преобразований множества возможных открытых (исходных) данных на множество возможных зашифро-

### Ш

ванных данных, осуществляемых по определенным правилам с применением ключей.

Калитлардан фойдаланган ҳолда алоҳида коидалар бўйича амалга ошириладиган, мумкин бўлган очиқ (дастлабки) маълумотлар тўпламини мумкин бўлган шифрланган маълумотлар тўпламига қайта ўзгартиришлар жами.

#### **Шифр абсолютно стойкий**

**uz** - абсолют барқарор шифр  
**en** - unbreakable cipher

Шифр, в котором знание шифротекста не позволяет улучшить оценку соответствующего открытого текста.

#### **Шифр аддитивный**

**uz** - аддитив шифр  
**en** - additive cipher

Шифрматни билиш, тегишли очиқ матн баҳоланишини яхшилаш имконини бермайдиган шифр.

Шифр гаммирования, в котором для наложения гаммы на данные используется бинарная операция аддитивного типа.

#### **Шифр асимметричный**

**uz** - асимметрик шифр  
**en** - asymmetric cipher

Гаммани маълумотларга қўйиш учун аддитив типдаги бинар операциядан фойдаланиладиган гаммалаш шифри.

Шифр, в котором ключ шифрования не совпадает с ключом дешифрования.

#### **Шифр блочный**

**uz** - блокли шифр  
**en** - block cipher

Шифрлаш калити дешифрлаш калити билан мос тўшмайдиган шифр.

1. Алгоритм шифрования, осуществляющий криптографическое преобразование исходной информации путем выполнения криптографических операций над  $n$ -битными блоками исходного или зашифрованного текста.

2. Шифр, входными текстами для которого являются блоки фиксированного размера.

### Ш

1. Дастлабки ёки шифрланган матннинг битли блоклари устида криптографик амалларни бажариш йўли билан дастлабки ахборотнинг криптографик алмаштирилишини амалга оширувчи шифрлаш алгоритми.

2. Кириш матнлари белгиланган ўлчамдаги блоклардан иборат бўлган шифр.

#### **Шифр гаммирования**

**uz** - гаммалаш

шифри

**en** - additive stream cipher

Потоковый шифр, в котором для зашифрования данных используется гаммирование.

Маълумотларни шифрлаш учун гаммалашдан фойдаланиладиган оқимли шифр.

#### **Шифр поточковый**

**uz** - оқимли шифр

**en** - stream cipher,

general stream cipher

Шифр, преобразующий последовательно отдельные биты или знаки открытого текста и ориентированный на реализацию в виде программы.

Очик матннинг кетма-кет айрим битларини ёки белгиларини ўзгартирувчи ва дастур кўринишида амалга ошириш учун мўлжалланган шифр.

#### **Шифр симметричный**

**uz** - симметрик

шифр

**en** - symmetric cipher

Шифр, являющийся, симметричной криптографической системой, т.е. использующий для зашифрования и расшифрования один и тот же ключ или такие различные ключи, что по одному из них легко может быть получен другой.

Симметрик криптографик тизим бўлган, яъни шифрлаш ва расшифровкалаш учун айнан бир калитдан ёки бири орқали бошқаси осон олинадиган турли калитлардан фойдаланиладиган шифр.

#### **Шифр составной**

**uz** - таркибли шифр

Шифр, составленный из нескольких более простых шифров, которые используются в

### Ш

en - product cipher

определенной последовательности при зашифровании и расшифровании данных.

Маълумотларни шифрлаш ва расшифровка-лашда маълум бир кетма-кетликда фойдаланиладиган бир нечта оддийрок бўлган шифрдан тузилган шифр.

**Шифр Файстеля**

uz - Файстел шифри

en - Facetel cipher

Специальный класс повторяющегося блочного шифра, в котором шифротекст вычисляется из открытого текста повторением применения функции обхода.

Такрорланадиган блокли шифрнинг махсус класси, унда шифр матн четлаб ўтиш функцияси қўлланишини такрорлаш билан очик матндан ҳисоблаб чиқилади.

**Шифратор**

uz - шифрлагич

en - encoder, cipher

Электронное устройство или программа, реализующая алгоритмы шифрования.

Шифрлаш алгоритмларини амалга оширадиган электрон курилма ёки дастур.

**Шифрование**

uz - шифрлаш

en - encryption

Способ обработки данных с использованием специальных алгоритмов, обеспечивающих их скрытую передачу. Преобразование информации осуществляется на уровне битов или их последовательностей в отличие от криптографических методов, где единицами кодирования обычно являются смысловые слова или фразы.

Маълумотларни, уларнинг яширин узатилишини таъминловчи махсус алгоритмлардан фойдаланиб, қайта ишлаш усули. Ахборотнинг ўзгартирилиши кодлаш бирликлари, одатда, мазмунли сўз ёки жумлалар бўлган криптографик методлардан фаркли ўларок, битлар ёки уларнинг кетма-кетлиги

### Ш

даражасида амалга оширилади.

#### **Шифрование абонентское**

**uz** - абонент шифрлаш  
**en** - end-to-end encryption

1. Криптографическая защита информации, передаваемой между двумя субъектами автоматизированной системы.

2. Защита информации, передаваемой средствами телекоммуникаций криптографическими методами, непосредственно между отправителем и получателем.

1. Автоматлаштирилган тизимнинг икки субъекти орасида узатиладиган ахборотнинг криптографик муҳофаза қилиниши.

2. Жўнатувчи ва олувчи ўртасида телекоммуникациялар воситалари ёрдамида бевосита узатиладиган ахборотнинг криптографик методлар билан муҳофаза қилиниши.

#### **Шифрование асимметричное**

**uz** - асимметрик шифрлаш  
**en** - asymmetric encryption

Метод засекречивания, при котором для шифрования применяются разные ключи.

Махфийлаштириш методи бўлиб, шифрлаш учун турли калитлардан фойдаланилади.

#### **Шифрование вероятностное**

**uz** - эҳтимолий шифрлаш  
**en** - probability encryption

1. Схема шифрования, в которой одному открытому тексту может соответствовать множество шифртекстов.

2. Процесс шифрования с использованием случайных параметров.

1. Битта очик матнга шифрматнлар тўплами тўғри келиши мумкин бўлган шифрлаш схемаси.

2. Тасодифий параметрлардан фойдаланган ҳолда шифрлаш жараёни.

#### **Шифрование методом Ривестра-Шамира-Адлемана**

**uz** - Ривестр-

Метод шифрования с открытым ключом, при котором ключ, используемый для шифрования, не совпадает с ключом для дешифрования (последний должен быть известен получателю).



### Ш

Шамир-Адлеман  
методи билан  
шифрлаш  
en - RSA encryption

**Шифрование одностороннее**  
uz - бир томонлама  
шифрлаш  
en - one-way  
encryption

**Шифрование сквозное**  
uz - очик шифрлаш  
en - end-to-end  
encryption, end-to-end  
encipherment

Очик калит билан шифрлаш методи бўлиб, шифрлаш учун фойдаланиладиган калит дешифрлаш учун мўлжалланган калит билан мос тушмайди (дешифрлаш калити олувчига маълум бўлиши керак).

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.*

Шифрлаш, дастлабки маълумотлари тикланиши мумкин бўлмаган шифрланган матн унинг натижаси ҳисобланади.

*Изоҳ: Бир томонлама шифрлаш аутентификация қилишида ишлатилади. Масалан, бир томонлама шифрлаш методи билан паролни шифрлаш натижасида олинган шифрланган матн сақланиб қолади. Кечроқ тақдим этилган пароль худди шу тарзда шифрланади. Кейин олинган иккала шифрланган матн солиштирилади, агар улар бир хил бўлса, унда тўғри пароль тақдим этилган.*

1. Метод засекречивания информации, при котором шифрованный поток передается через сеть в прозрачном режиме, т.е. без перешифрования трафика в промежуточных узлах телекоммуникаций.

2. Шифрование данных в пределах системы или на стороне источника с соответствующим дешифрованием, которое осуществляется только в пределах системы или на стороне назначения.

### Ш

1. Ахборотни махфийлаштириш методи бўлиб, шифрланган оқим тармоқ орқали очик режимда, яъни трафик оралик телекоммуникациялар узелларида қайта шифрламасдан узатилади.

2. Маълумотларни тизим доирасида ёки тегишлича дешифрлаш билан манба томонда шифрлаш. Фақат тизим доирасида ёки мўлжалланган томонда амалга оширилади.

#### **Шифрование с открытым ключом**

**uz** - очик калит билан шифрлаш  
**en** - public key cryptography

Криптографический метод, в котором используется открытый ключ для формирования шифротекста и закрытый ключ для преобразования шифротекста в исходный текст.

Криптографик метод бўлиб, шифрматни тузиш учун очик калитдан, шифрматни дастлабки матнга ўзгартириш учун эса ёпик калитдан фойдаланилади.

#### **Шифросистема**

**uz** - шифрtizим  
**en** - cryptosystem

Криптографическая система, обеспечивающая конфиденциальность информации путем ее шифрования.

Шифрлаш йўли билан ахборотнинг конфиденциаллигини таъминлайдиган криптографик тизим.

#### **Шифротекст**

**uz** - шифр матн  
**en** - ciphertext

Результат зашифрования исходного открытого текста, осуществляемого с целью сокрытия его смысла.

Дастлабки очик матни, унинг маъносини яшириш мақсадида амалга ошириладиган, шифрматнга ўгириш натижаси.

#### **Шлюз двухпортовый**

**uz** - икки портли шлюз  
**en** - dual-homed

Компьютер, на котором работает программное обеспечение межсетевое экрана и который имеет две сетевых карты: одна подключена к внутренней сети, а вторая – к внешней. Шлюз передает информацию из

### Ш

gateway

одной сети в другую, исключая прямое взаимодействие между ними.

Тармоқлараро экран дастурий таъминоти ишлайдиган ва иккита – бири ички тармоққа, иккинчиси ташқи тармоққа уланган тармоқ карталарига эга бўлган компьютер. Шлюз ахборотни бир тармоқдан иккинчисига, улар ўртасида бевосита ўзаро таъсирни истисно қилган ҳолда узатади.

**Шлюз прикладного уровня**  
**uz** - амалий даражадаги шлюз  
**en** - application-level gateway

Один из вариантов реализации межсетевое экрана, который исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Фильтрация всех входящих и исходящих пакетов осуществляется на прикладном уровне эталонной модели ВОС. Связанные с приложениями программы-посредники перенаправляют через шлюз информацию, генерируемую конкретными сервисами TCP/IP.

Тармоқлараро экранни амалга ошириш вариантларидан бири. Муаллифлаштирилган мижоз билан ташқи хост ўртасида бевосита ўзаро таъсирни истисно қилади. Барча қирадиган ва чиқадиган пакетлар фильтрацияси ВОС эталон моделининг амалий даражасида амалга оширилади. Иловалар билан боғланган воситачи дастурлар шлюз орқали TCP/IP муайян сервислари генерациялайдиган ахборотни қайта йўллайди.

**Шлюз сеансового уровня**  
**uz** - сеанс даражасидаги шлюз  
**en** - circuit-level gateway

Один из вариантов реализации межсетевое экрана, который исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Принимает запрос доверенного клиента на определенные услуги и, после проверки прав доступа на запрошенный сеанс, устанавливает соединение с

### Ш

внешним хостом. После этого шлюз копирует пакеты в обоих направлениях, не осуществляя их фильтрации.

Тармоқлараро экранни амалга ошириш вариантларидан бири. Муаллифлаштирилган миждоз билан ташки хост ўртасида бевосита ўзаро ҳамкорликни истисно қилади. Ваколатли миждознинг муайян хизматларга бўлган сўровини қабул қилади, сўралган сеансга қира олиш ҳуқуқи текширилгандан сўнг, ташки хост билан боғланишни амалга оширади. Бундан кейин шлюз пакетлар фильтрациясини бажармасдан, иккала йўналишда бу пакетлардан нусха олади.

### Э

#### Экспозиция

uz - экспозиция

en - exposition

Форма возможной потери или ущерба для системы. Например, экспозициями считаются неавторизованный доступ к данным или противодействие авторизованному использованию системы.

Тизим учун мумкин бўлган йўқотишлар ёки зарар шакли. Масалан, маълумотлардан муаллифлаштирилмаган тарзда эркин фойдаланиш ёки тизимдан муаллифлаштирилган тарзда фойдаланишга қарши туриш экспозиция ҳисобланади.

#### Экранирование

uz - экранлаш

en - screening

1. Функция межсетевого экрана, позволяющая поддерживать безопасность объектов внутренней области, игнорируя несанкционированные запросы из внешней области.  
2. Разграничение межсетевого доступа путем фильтрации передаваемых данных.

1. Тармоқлараро экраннинг, ташки соҳадан

бўладиган рухсат этилмаган сўровларни рад қилган ҳолда, ички соҳа объектларининг хавфсизлигини таъминлайдиган функцияси.

2. Узатиладиган маълумотларни филтрлаш йўли билан тармоқлараро эркин фойдаланиш (кириш) чегараларини белгилаш.

**Экран межсетевой  
uz - тармоқлараро  
экран  
en - firewall**

1. Локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство, реализующее контроль за информацией, поступающей в систему и/или выходящий из системы.

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

1. Тизимга келиб тушадиган ва ёки тизимдан чиқиб кетадиган ахборотнинг назорат қилинишини амалга оширадиган локал ёки (бир компонентли) функционал тақсимланган дастурий (дастурий-аппарат) восита.

2. Икки тармоқ туташган ерда ўрнатиладиган ва бир тармоқни бошқа бир тармоқда айланадиган трафикдан муҳофазаловчи ҳимоя воситаси; ташқаридан бўладиган хужумларнинг олдини олиш учун хизмат қилади.

**Экран межсетевой  
с фильтрацией  
пакетов  
uz - пакетлар филт-  
рланадиган  
тармоқлараро экран  
en - packet-filtering  
firewall**

Один из вариантов реализации межсетевого экрана. Исключает прямое взаимодействие между авторизованным клиентом и внешним хостом путем фильтрации входящих и исходящих пакетов. Фильтрация осуществляется на основе информации, содержащейся в заголовке пакета (адреса отправителя и получателя, номера портов и т.п.).

Тармоқлараро экранни амалга ошириш ва-

риантларидан бири. Муаллифлаштирилган мижоз билан ташқи хост ўртасида кирувчи ва чиқувчи пакетларни филтрлаш орқали бевосита ўзаро таъсирни истисно қилади. Филтрлаш пакет Сарлавҳасидаги ахборот асосида (жўнатувчи ва олувчи адреслари, порт номерлари ва ш.к.) амалга оширилади.

**Эксплойт**  
uz - эксплойт  
en - exploit

Вредоносный код, эксплуатирующий уязвимости программных компонентов компьютера.

Компьютер дастурий компонентларининг заиф томонларидан фойдаланадиган зарарли код.

**Энтропия**  
uz - энтропия  
en - entrophy

В теории информации – мера неопределенности состояния объекта или некоторой ситуации (случайной величины) с конечным числом исходов. Понятие энтропии введено Шенноном и используется для определения количества информации в сообщении.

Ахборот назариясида – объект ҳолатининг ёки қандайдир вазиятнинг (тасодифий катталикнинг) ноаниқлик ўлчови. Энтропия тушунчаси Шеннон томонидан киритилган ва ундан хабардаги ахборотнинг микдорини аниқлаш учун фойдаланилади.

**Этикетка авторская**  
uz - муаллифлик ёрлиғи  
en - copyright notice

Уведомление об авторском праве на программный продукт, обычно включается в начало программного листинга и обязательно отображается на дисплее компьютера.

Дастурий маҳсулотга бўлган муаллифлик ҳуқуқи тўғрисидаги билдиришнома. Одатда, дастурий листинг бошланишида киритилади ва компьютер дисплейида акс эттирилади.

**Эффективность**

1. Степень соответствия достигнутых ре-

## Э

**защиты информации**

**uz** - ахборотни муҳофаза қилиш самарадорлиги

**en** - information technical protection efficiency

зультатов действий по защите информации поставленной цели защиты.

2. Показатель, характеризующий уровень технической защиты информации.

1. Ахборотни муҳофаза қилиш бўйича эришилган иш натижаларининг қўйилган мақсадга мувофиқ келиш даражаси.

2. Ахборотни техник муҳофаза қилиш даражасини тавсифловчи кўрсаткич.

## Я

**Ядро безопасности**

**uz** - ҳавфсизлик ядроси

**en** - security kernel

Программные и аппаратные элементы достоверной вычислительной базы (ДВБ), реализующие концепцию монитора ссылок. Они должны разделять все попытки доступа субъектов к объектам, быть защищенными от модификации и проверены на корректное выполнение своих функций.

Ишончли ҳисоблаш базаси (ИХБ) нинг ҳаволалар монитори концепциясини амалга оширадиган дастурий ва аппарат элементлари. Улар субъектларнинг объектлардан эркин фойдаланишга бўлган барча уринишларини ажратиши, ўзгартиришлардан муҳофазаланган бўлиши ва ўз функцияларини тўлақонли бажариш юзасидан текширилиши керак.

**Ядро защиты**

**uz** - муҳофаза ядроси

**en** - security kernel

Технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа.

Муҳофаза қилиш воситалари комплексининг эркин фойдаланиш (кириш) диспетчери концепциясини амалга оширадиган техник, дастурий ва микродастурий элементлари.

## Я

### **Язык администрирования базы данных**

**uz** - маълумотлар базасини бошқариш тили  
**en** - database administration language

Искусственный язык для описания действий, связанных с администрированием базы данных.

Маълумотлар базасини бошқариш билан боғлиқ бўлган ишларни тавсифлаш учун мўлжалланган сунъий тил.

### **Язык базы данных**

**uz** - маълумотлар базаси тили  
**en** - database language

Искусственный язык для описания процессов создания, ведения и использования баз данных.

Маълумотлар базасини яратиш, олиб бориш ва ундан фойдаланиш жараёнларини тавсифлаш учун мўлжалланган сунъий тил.

### **Язык гипертекстовой разметки документов**

**uz** - хужжатларни гиперматнли белгилаш тили  
**en** - hypertext markup language, HTML

1. Язык, используемый для создания веб-страниц.

2. Способ описания документов в WWW. Язык HTML использует набор тегов, вводимых в текстовые документы, которые указывают браузеру или другой программе, каким образом информация должна выводиться на экран.

1. Веб-саҳифаларни яратиш учун фойдаланиладиган тил.

2. Хужжатларни WWW да тавсифлаш усули. HTML тили матнли хужжатларга кириладиغان, браузер ёки бошқа дастурга ахборот экранга қай тарзда чиқарилишини кўрсатадиган теглар тўпламидан фойдаланади.

### **Язык запросов**

**uz** - сўровлар тили  
**en** - query language

Искусственный язык для описания запросов, поиска данных в базах данных и действий над запросами.



## Я

Сўровларни тавсифлаш, маълумотлар базадасида маълумотларни излаб топиш, сўровлар устида амаллар бажариш учун мўлжалланган сунъий тил.

### Язык Java

uz - Java тили

en - Java language

Новый язык программирования, разработанный Sun Microsystems, Inc. Язык Java может использоваться как обычный язык программирования для разработки сетевых приложений, а также для написания небольших приложений, называемых апплетами.

Sun Microsystems, Inc томонидан ишлаб чиқилган янги дастурлаш тили. Java тилидан тармоқ иловаларини (дастурларини) ишлаб чиқиш учун оддий дастурлаш тили сифатида, шунингдек, апплетлар деб аталадиган унча катта бўлмаган иловаларни ёзишда фойдаланилади.

## Содержание

|   |   |
|---|---|
| Введение .....  | 3 |
| Русско-узбекский толковый словарь терминов по информационной безопасности ..... | 5 |

## Мундарижа

|  |   |
|--|---|
| Кириш .....  | 4 |
| Ахборот хавфсизлигига оид атамаларнинг русча-ўзбекча изоҳли луғати ..... | 5 |

**РУССКО-УЗБЕКСКИЙ ТОЛКОВЫЙ СЛОВАРЬ  
ТЕРМИНОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

---

**АХБОРОТ ХАВФСИЗЛИГИГА ОИД ТЕРМИНЛАРНИНГ  
РУСЧА-ЎЗБЕКЧА ИЗОҲЛИ ЛУФАТИ**

*Ўзбекистон Алоқа ва ахборотлаштириш агентлиги  
Илмий-техник ва маркетинг тадқиқотлари маркази  
Илмий кенгаши томонида нашрга тавсия этилган*

*Муҳаррирлар: А.С. Михерева, А. Шаропов  
Мусаҳҳиҳлар: К. Загряжская, М. Саидова  
Техмуҳаррир: Н.В. Тимофеева*

Нашриёт раками 3-124. Теришга берилди 20.07.2009. Босишга рухсат  
этилди 06.08.2009. Формат 60x84 1/16. Ҳисоб-нашриёт т. 18,0. Адади  
500 нусхада. 152 буюртма. Баҳоси келишилган нарҳда.

Ўзбекистон Республикаси ФА «Фан» нашриёти  
100170, Тошкент, И. Мўминов кўчаси, 9-уй.

«КО‘НИ-NUR» МЧЖ босмахонасида чоп этилди.  
Тошкент шаҳри, «Машинасозлар» мавзеси, 4-уй.

