

УКАЗАТЕЛЬ АНГЛОЯЗЫЧНЫХ ТЕРМИНОВ

A

- abonent, 7
- above the application layer cryptographic mechanisms, 224
- access, 58
- access control, 263
- access control list, 221
- access control mechanism, 118
- access control service, 278
- access matrix, 110
- access structure, 238
- access to information, 58
- access type, 247
- accessibility, 61
- accountability, 149
- accreditation, 7
- active adversary, 124, 175
- active attack, 16
- active audit, 23
- active threat, 249
- adaptive attack, 15
- adaptive chosen-ciphertext attack, 15
- adaptive chosen-plaintext attack, 15
- additional cryptographic mechanisms, 224
- adequacy, 58
- administrative regulation, 186
- advanced electronic signature, 159
- adversary, 175
- advertising-supported software, 132
- adware, 132
- AES (Advanced Encryption Standard), 234
- AIS (Automated Information System), 204
- anonymity, 14
- anonymizer, 13
- anti bot, 14
- antivirus, 172
- application control, 266
- application control default deny, 100
- application cryptographic protocol, 178
- application layer cryptographic mechanisms, 224
- arbiter, 14
- arbitrated protocol, 180
- arbitration, 15
- asset, 8
- assurance, 53
- asymmetric cryptosystem, 290
- attack, 15
- attack on computer network, 20
- attack on the cryptosystem, 17
- attack on the protocol, 19
- attack potential, 165
- attacker, 123
- audit, 186

А УКАЗАТЕЛЬ АНГЛОЯЗЫЧНЫХ ТЕРМИНОВ

audit trail, 213
auditability, 155
authenticated communication channel, 91
authentication, 24
authentication code, 97
authenticity, 28
authorised use, 163
authority, 281
authorization, 7
authorized access
to information, 59
autocorrelation test, 245
automated system, 202
availability, 61

В

backdoors, 214
balanced sequence, 164
baseline controls, 112
basic block encryption algorithm, 9
basic strength of function, 238
battery of tests, 122
bimetric authentication, 25
binary key, 95
birthday attack, 115
bit commitment protocol (scheme), 176
black box assumption, 166
black-box, 294
blind digital signature, 156
blind signature scheme, 241
block ciphering system, 290
boot virus, 40
bootkit, 37

bot, 36
botnet, 36
breaking of cryptosystem, 52
browser hijacking, 75
brute-force attack, 17, 115
bug, 28, 64
build-in cryptographic mechanisms, 224
BYOD (Bring Your Own Device), 61

С

Carberp, 93
carding, 93
cardseller, 94
cash machine, 28
cash-in terminal, 244
CBA (Certificate-Based Authentication), 26
certificate, 195
certification, 197
certification center, 282
certification service provider, 171
channel, 91
checksum, 239
cipher, 213, 288
ciphering sequence, 48
ciphertext, 219, 244, 291
ciphertext-only attack, 17
classified information, 81
classifying information, 94
cleartext, 219
CMF (Content Monitoring and Filtering), 211
coin flipping (by telephone) protocol, 179

- collision, 99
- collision-intractable hash function, 280
- combining function, 276
- commercial information, 84
- communication and consultation, 134
- communication channel, 91
- communication complexity, 215
- communication facilities, 227
- communication network, 201
- communication security, 33
- commutation key, 96
- complete packet inspection, 246
- completeness property, 162
- complexity-based security, 237
- composite key, 97
- compression function, 276
- compromise, 99
- compromised key, 97
- computer, 100
- computer attack, 16
- computer crime, 167
- computer cryptography, 105
- computer network, 200
- computer resource, 188
- computer security, 32
- computer security evaluation, 151
- computer system, 206
- computer system security, 34
- computer virus, 40
- Conficker, 103
- confidentiality, 102
- confusion property, 194
- confusion transform, 167
- connection integrity service with recovery, 278
- connection integrity service without recovery, 278
- consequence, 164
- context-based authentication, 26
- contract signing protocol, 179
- control, 112
- control sequence, 164
- controllable territory, 71
- correlation attack, 16
- correlation cryptanalysis, 114
- correlation of functions, 104
- covert channel, 92
- covert channel capacity, 175
- covert statistical channel, 92
- covert storage channel, 92
- covert timing channel, 92
- crimeware, 132
- critical structures, 238
- cryptanalysis, 104
- cryptanalysis based on collision search, 114
- cryptanalyst, 104
- cryptanalytic assumptions, 166
- crypt-analytic method, 114
- crypto API (application programming interface), 104
- cryptofilter, 106
- cryptogram, 104
- cryptographic algorithm, 10
- cryptographic assumption, 166
- cryptographic device, 269
- cryptographic function, 275
- cryptographic hardware, 224

С УКАЗАТЕЛЬ АНГЛОЯЗЫЧНЫХ ТЕРМИНОВ

cryptographic hash function, 279
cryptographic hash function with key, 279
cryptographic information protection facility, 229
cryptographic key disclosure, 99
cryptographic mechanisms, 224
cryptographic operation, 145
cryptographic primitive, 167
cryptographic protection, 69
cryptographic protection of information, 67
cryptographic protocol, 178
cryptographic security, 236
cryptographic service, 274
cryptographic services, 226
cryptographic system (cryptosystem), 206
cryptographic tools, 224, 228
cryptographically strong pseudorandom bit generator, 49
cryptographically strong pseudorandom sequence, 164
cryptography, 104
cryptology (mathematical cryptography), 105
cryptoprotocol, 106
cryptoprotocol, 106
cryptoprotocol, 106
cryptorouter, 105
cryptoserver, 106
cryptosynthesis, 201
cryptosystem, 206, 213
CSRF (Cross-Site Request Forgery), 154
cyber crime, 94

cyber terrorism, 94
cyberspace, 175

D

damage, 271
data, 49
data block, 34
data confidentiality service, 277
data deciphering, 186
data encryption key, 97
data integrity, 280
data integrity service, 278
data medium, 128
data origin authentication, 25
data origin authentication service, 277
data privacy, 194
data protection, 66
data protection Directive 95/46/EC, 52
data security, 29
data transfer system, 213
data transmission channel, 91
database, 28
DDoS (Distributed Denial-of-Service attack), 18
deciphering, 10, 186
decryption, 52, 186
decryption algorithm, 10
decryption function, 276
decryption key, 96
defacement, 53
denial of service, 149
deposit transaction (protocol), 247
DES (Data Encryption Standard), 234

destruction, 184
dictionary attack, 20
differential attack, 20
differential cryptanalysis, 114
differential fault attack, 20
differential-linear attack, 20
Diffie-Hellman algorithm, 176
diffusion property, 194
diffusion transform, 167
digiCash, 51
digital fingerprint, 279
digital information, 84
digital money, 51
digital signature, 155
digital signature cryptosystem, 210
digital signature scheme, 240
digital signature with message recovery, 156
digram, 34
Directive 1999/93/EC, 52
discrete logarithm problem, 63
discretionary access control, 168, 264
dishonest party, 124
distribution of information, 166
DLP (Data Loss Prevention, Data Leak Prevention), 211
document, 55
DoS attack (Denial-of-Service attack), 17
DPL (Deep Packet Inspection), 246
Dropper, 62
DSS (Digital Signature Standard), 233

E

eavesdropper, 125, 176
e-cash, 51
e-cash system, 202
e-coin, 51, 121
EDI (Electronic Data Interchange), 208
EES (Escrowed Encryption Standard), 235
efficiency, 294
EFT (Electronic Funds Transfer), 209
El Gamal digital signature scheme, 242
election scheme, 177
electronic cash system, 202
electronic data, 81
electronic message, 56, 219
electronic money, 51
electronic passport, 152
electronic payment system, 209
electronic signature, 156
electronic signature facility certificate, 197
e-money, 51
e-money double spending problem, 171
enciphering, 288
enciphering key, 96
encryption algorithm, 9, 11
encryption function, 275, 277
encryption method (cipher type), 221
encryption mode, 187
encryption, 288
end-point encryption, 289

Е УКАЗАТЕЛЬ АНГЛОЯЗЫЧНЫХ ТЕРМИНОВ

enterprise information system, 205
entity, 270
entity authentication, 27
EPS (Extrusion Prevention System), 211
equivalent keys, 97
equivalent keys attack, 17
equivalent keys cryptanalysis, 114
ER&A (Entity Resolution and Analysis), 184
establishing the context, 269
evaluation assurance level, 268
evaluation authority, 146
evaluation, 151
event, 216
e-wallet, 37
exhaustive key search, 115
existential collision, 99
existential forgery, 155
exploit, 293
exposure, 154

F

fail-stop signature scheme, 242
fair blind signature scheme, 241
faulttolerant system, 209
Feistel scheme, 243
filtering function, 277
firewall, 291
FMS (Fraud Management System), 14
forgery, 154
fork bomb, 38
formal, 274
fraud, 274

frequency, 286
frequency cryptanalysis, 116
frequency test, 246
full disk encryption, 289
function with interdictions, 276
functional object, 138
function-to-function distance, 186

G

Golomb postulates, 165
GOST 28147-89, 234
GOST digital signature algorithm P 34.10-2001, 233
GOST digital signature algorithm P 34.10-2012, 233
GOST digital signature algorithm P 34.10-94, 233
GOST hash function P 34.11-2012, 234
GOST hash function P 34.11-94, 234
group digital signature, 156
group signature protocol, 179
group signature scheme, 241
group-oriented protocol, 177
guideline, 190
guidelines, 187

H

hacker, 279
hardware, 223
hardware encryption, 289
hash, 279
hash function, 279
hash-code, 279

hashing algorithm, 10

hash-result, 279

hash-value, 279

hazard, 144

hierarchy of keys, 74

high strength of function, 238

honest party, 270

honest-verifier zero-
knowledge, 183

honey pot, 138

I

I&A (Identification and
Authentication), 73

IAM (Identity and Access
Management), 265

ICT security, 32

ICT security policy, 160

ideal random sequence, 164

ideal secret sharing scheme, 242

identification, 72

identification protocol, 177

identification scheme, 240

identification system, 204

identifier, 72

identity, 50

Identity Awareness, 148

IdM (Identity Management), 264

IDS (Intrusion Detection
System), 208

illegal access, 60

imitation, 75

imitation resistance, 76

imprint, 279

inside intrusion, 48

incident, 85

informal, 128

information, 79

information assets, 9

information assets
confidentiality, 102

information assets integrity, 280

information availability, 62

information dissemination, 185

information environment, 222

information flow control, 266

information hiding, 218

information infrastructure, 84

information integrity
violation, 124

information leakage channel, 93

information loss, 270

information object, 137

information objects, 139

information owner, 42

information process, 181

information processing, 135

information processing
facility(ies), 232

information processing
system, 209

information protection
measure, 112

information risk assessment, 151

information security, 30

information security
concept, 103

information security event, 217

information security incident, 85

information security intruder
model, 119

information security measure, 113

I УКАЗАТЕЛЬ АНГЛОЯЗЫЧНЫХ ТЕРМИНОВ

information security
monitoring, 121
information security
threat, 120, 250
information security threat-risk
model, 120
information security
vulnerability, 272
information sphere, 239
information system, 204
information target, 137
information technical protection
facilities, 228
information technology, 246
information technology
security, 34
information technology security
evaluation criteria, 107
information war, 46
information weapon, 148
information with restricted
access, 82
information-telecommunication
system, 205
information-theoretic (Shannon)
security, 237
informatization, 79
information resource, 187
infrastructure, 84
initialization vector, 37
insecurity channel, 91
inside adversary, 125
insider, 76
integer factoring problem, 64
integrity, 280
integrity check value, 98

integrity protection, 76
integrity protection algorithm, 9
integrity system, 204
interactive authentication, 25
interactive proof, 54
interactive protocol, 178
interdiction free function, 275
international cyber crime, 167
internet fraud, 78
intruder model, 119
intrusion, 47
involution encryption
algorithm, 11
IPC (Information Protection and
Control), 211
IPC (Information Protection and
Control), 66
IPS (Intrusion Prevention
System), 210
IRM (Information Rights
Management), 266
ISOC (Information Security
Operation Center), 285
isolated communication
networks, 198
iterative encryption algorithm, 11
IX (Information eXtraction), 246

К
KEK (Key Enciphering Key), 97
Kerckhoffs assumption, 165
key (of a cryptosystem), 95
key certificate, 195
key distribution center, 282
key distribution protocol, 180
key escrow, 51

key establishment system, 213
key generator, 48
key gun, 63
key identifier, 72
key length, 53
key life period, 47
key life time, 47
key lifetime, 286
key management system, 212
key scheduling, 182
key sequence, 48
key set (of a cryptosystem), 119
key stream, 163
key system, 206
key updating, 135
keylogger, 94
keystream, 48
keystream cipher, 288
known plaintext attack, 17

L

latin square, 94
least privilege, 118
legal user, 162
level of risk, 268
license, 109
likelihood, 46
linear attack, 17
linear complexity profile test, 245
lock out, 65
logic bomb, 35
long-term key, 96
loophole, 108

M

macro viruses, 109

mail bomb, 36
malicious logic, 64
malicious software, 130
malware, 130
management, 111
mandatory access control, 264
man-in-the-middle, 287
man-in-the-middle attack, 21
manipulation detection, 269
mapping free of error
propagation, 150
maskerade, 110
master key, 95
Maurer universal test, 245
MDM (Mobile Device
Management), 266
medium strength of function, 238
meet-in-the-middle attack, 21
memory using attack, 19
memory using cryptanalysis, 116
memory-used search attack, 19
message, 219
message authentication, 27
message authentication code, 75
message authentication code, 98
message authentication code
mode, 187
message authentication
protocol, 177
message digest, 279
message integrity, 281
method of cryptanalysis, 114
mixing property, 194
mixing transform, 166
model, 119
mandatory access control, 168

monitoring, 121
moving probable word
attack, 20
moving probable word
cryptanalysis, 115
multilevel security, 69
multiple digital signature, 156
multi-factor authentication, 26
mutual authentication, 25

N

national security concept, 104
NCSC (National Computer
Security Center), 127
network attack, 20
network layer cryptographic
mechanisms, 225
network scanner, 213
network security, 33
network security scanner, 213
network traffic, 248
network worm, 287
next bit test (predictor), 245
nondegenerate function, 276
noninteractive zero-knowledge
proof, 55
nonqualified electronic
signature, 158
non-repudiation, 127
non-repudiation of origin, 127
non-repudiation service, 278
non-repudiation service with
proof of delivery, 278
non-repudiation service with
proof of origin, 278
notarization, 129

O

object, 136
object reuse, 87
official standard, 233
off-line e-cash system, 209
once-only key, 96
one-click attack, 154
one-click attack или session
riding, 154
one-time digital signature, 156
one-time pad, 35
one-time padding, 48
one-way authentication, 27
one-way permutation, 159
on-line e-cash system, 209
open security, 32
open source, 98
open standard, 232
organizational information
security policies, 160
organizational security
policies, 160
OTP (One-Time Password), 152
OTP authentication (One-Time
Password authentication), 26
OTP OOB (One-Time Passwords
Out-Of-Band), 152
outside adversary, 125
OWHF (one-way hash
function), 279
owner of information, 134
owner of signature verification
key certificate, 42

P

P2P (Peer-to-Peer network), 201

- packet filtering, 272
- party, 270
- pass (of cryptographic protocol), 286
- passive adversary, 125, 176
- passive attack, 19
- passive threat, 251
- password, 26, 152
- password attack, 21
- password cracker, 47
- password cracking, 39
- payment transaction (protocol), 247
- peer entity authentication service, 277
- penetration, 175
- perfect cipher, 288
- perfect secrecy, 236
- perfect secret sharing scheme, 242
- perfect zero-knowledge proof, 55
- permutation cipher, 288
- personal data, 50
- personal data dissemination, 185
- personal data processing, 135
- personal data protection, 29
- personal data transborder transmission, 152
- phishing, 273
- physical and data layer cryptographic mechanisms, 226
- physical security, 69
- PKI (Public Key Infrastructure), 85
- plain text model, 120
- plaintext, 219, 244
- polymorphic viruses, 41
- practical security (of the cryptosystem), 236
- preliminary key distribution scheme, 242
- primitive cryptographic protocol, 178
- privacy, 102, 243
- private communication channel, 91
- private-key cryptosystem, 290
- privilege matrix, 221
- privilege violation, 124
- product, 175
- program, 173
- program bug, 64
- program verification, 38
- program viability, 63
- proof of knowledge, 54
- proprietary standard, 232
- protected automated system, 203
- protected information resource, 188
- protection class of computer system, 95
- protection continuity, 128
- protection criterion of computer system, 160
- protection facility, 229
- protection from imitation, 76
- protection from unauthorized access, 68
- protection level certification, 198
- protection model, 119
- protection of information, 66

Р УКАЗАТЕЛЬ АНГЛОЯЗЫЧНЫХ ТЕРМИНОВ

protection profile, 181
protection, 65
protocol, 176
protocol action, 287
provable security, 236
pseudorandom function family, 194
pseudorandom function generator, 49
pseudorandom generator, 49
pseudorandom permutation family, 194
pseudorandom permutation generator, 48
pseudo-random sequence, 163
public key, 96
public key distribution, 184
public personal data, 50
public-key cryptosystem, 290
PUPs (Potentially Unwanted Programs), 174

Q

qualified certificate, 195
qualified electronic signature, 157
quality of service, 94
quantum cryptanalysis, 104
quantum cryptographic protocol, 178
quantum cryptographic system, 207
quantum cryptography, 105
quantum key distribution, 184
quantum pseudorandom generator, 49

R

ransomware attack, 16
recovering, 47
recurrent sequence, 164
reference monitor, 121
reference monitor concept, 103
reference validation mechanism, 118
registration center, 282
reliability, 58, 123
replay attack, 19
repudiation, 150
residual risk, 190
resource, 187
restricted access, 61
review, 153
risk, 188
risk acceptance, 170
risk aggregation, 7
risk analysis, 12
risk assessment, 151
risk attitude, 149
risk aversion, 128
risk avoidance, 262
risk control, 100
risk criteria, 107
risk description, 145
risk evaluation, 150
risk financing, 273
risk identification, 73
risk management, 111, 267
risk management audit, 24
risk management framework, 211
risk management plan, 153
risk management policy, 161
risk management process, 181

- risk matrix, 110
 - risk owner, 42
 - risk perception, 47
 - risk profile, 181
 - risk register, 186
 - risk reporting, 150
 - risk retention, 262
 - risk sharing, 184
 - risk source, 88
 - risk tolerance, 247
 - risk treatment, 45, 135
 - role, 190
 - rootkit, 191
 - round (of cryptographic protocol), 286
 - round key, 97
 - RSA cryptosystem, 290
 - RSA encryption algorithm, 11
 - run test, 245
 - running key ciphering, 48
- S**
- safeguard, 111
 - scrambler, 214
 - seal, 98
 - second preimage resistant hash function, 280
 - secret exchange protocol, 178
 - secret key, 96
 - secret key cryptosystem, 290
 - secret share, 56
 - secret sharing, 242
 - secret sharing protocol, 179
 - secure electronic signature devices, 226
 - secure messaging encryption, 195
 - secure operating system, 145
 - secure state, 220
 - secure-signature-creation device, 270
 - security, 29
 - security administrator, 7
 - security attribute, 21
 - security audit, 23
 - security evaluation, 151
 - security flaw, 37
 - security function, 275
 - security function policy, 161
 - security goal, 281
 - security kernel, 53, 294
 - security label, 113
 - security objective, 281
 - Security Operation Center, 284
 - security policy, 165
 - security policy model, 119
 - security policy realization, 211
 - security policy violator, 125
 - security policy violator's model, 119
 - security service, 269
 - security services, 277
 - security system violation, 124
 - security target, 63
 - security violation, 124
 - selective field integrity, 280
 - selective forgery, 154
 - self-service cash-in terminal, 244
 - SEM (Security Event Management), 267
 - semiformal, 162
 - sender authentication, 27

S УКАЗАТЕЛЬ АНГЛОЯЗЫЧНЫХ ТЕРМИНОВ

- sensitive information, 84
- sensitivity label, 113
- sequential key search, 19, 115
- serial test, 246
- sertification authority, 282
- service, 278
- session encryption, 289
- session key, 96
- session riding, 154
- share, 56
- shared access, 60
- SHS (Secure Hash Standard), 234
- SIEM (Security Information and Event Management), 191
- signature creation data, 97
- signature generation algorithm, 9
- signature space, 175
- signature verification algorithm, 10
- signature verification data, 96
- SIM (Security Information Management), 265
- Simmons authentication theory, 244
- skimming, 213
- sniffer, 216
- sniffers, 13
- sniffing, 216
- SOC, 284
- social engineering, 76
- software, 130
- software cryptographic mechanisms, 225
- software dissemination, 185
- software encryption, 289
- software modification, 120
- software security module, 230
- space complexity, 216
- spam, 220
- spoofing, 222
- spoofing attack, 17
- spyware, 133
- SQL injection, 86
- SSCD (secure signature creation device), 270
- SSO (Single Sign-On), 7
- standard, 232
- standardization, 187, 235
- standardization guidelines, 187
- statistical cryptanalysis, 115
- step (of a protocol), 287
- stream cipher, 9
- stream cipher ciphering module, 121
- stream cipher control module, 120
- stream ciphering system, 290
- stream encryption algorithm, 9
- strength of function, 238
- subject, 239
- subscriber, 7
- substitution, 155
- substitution cipher, 288
- symmetric cryptosystem, 290
- synchrosignal, 202
- system availability, 49
- system of protection from unauthorized access to information, 203
- system security, 34
- system, 202

T

target of protection, 137
TCB (Trusted Computing Base), 57, 99
technical regulation, 186
telecommunication, 244
telecommunication facilities, 227
telecommunication system, 212
text block, 35
theoretical security, 236
threat, 249
threat management, 267
threat types, 39
threshold cryptographic scheme, 207
threshold secret sharing scheme, 242
time complexity, 215
timestamp, 113
timestamping authority, 285
TOE (Target of Evaluation), 138
TOE resource, 188
TOE security functions, 275
TOE security functions interface, 79
TOE security policy, 161
TOE security policy model, 120
TOR (The Onion Router), 198
traffic (flaw) confidentiality, 102
traffic, 248
traffic analysis, 13
traffic padding, 118
transform free of error propagation, 167
transport layer cryptographic mechanisms, 225

trapdoor function, 276
trapdoor function generator, 49
trapdoor permutation family, 194
trapdoors, 214
treat-risk model, 120
trojan, 173, 248
trojan horse, 173, 248
true random sequence, 163
trusted authority, 281
trusted channel, 91
trusted entity, 281
trusted functionality, 275
trusted path, 110
trusted third party, 281
tunnelling, 248
two-factor authentication, 25
two-party protocol, 177

U

unauthorized access, 60
unauthorized access to information, 59
unauthorized user, 162
unclassified information, 81
undeniable digital signature, 156
undeniable signature scheme, 241
unicity distance, 186
unintentional denial-of-service, 18
universal forgery, 154
unlinkability, 128
untraceability, 128
unwanted software, 174
URLF (URL filtering), 273

У УКАЗАТЕЛЬ АНГЛОЯЗЫЧНЫХ ТЕРМИНОВ

user, 162
user authentication, 24
user data, 50
user identification in an information system, 73
user of signature verification key certificate, 162
UTM (Unified Threat Management), 268

V

V&V (Verification and Validation), 38
vaccination, 37
validator, 122
validity, 58
verifiable secret sharing, 183
verifiable secret sharing protocol, 180
verification, 38
viability, 63
virtual money, 50
virus, 40
voting protocol, 177
voting scheme, 177
VPN (virtual private network), 199
vulnerability, 271
vulnerability management, 268

W

wallet, 37
weak key, 97
web-anonymizer, 37
weight of boolean function, 38
white book, 34

withdrawal transaction (protocol), 148

X

XSRF (Cross-Site Request Forgery), 154
XSS (Cross-Site Scripting), 110

Z

zero day attack, 19
zero day exploit, 272
zero-knowledge identification, 73
zero-knowledge proof, 55
zero-knowledge property, 183
Zeus, 71