

Краткий толковый словарь
по информационной безопасности

версия 1.0

1000 терминов

Москва, 2000

Предисловие

Данный толковый словарь является одной из первых попыток разработать единую терминологию в области информационной безопасности. Этот документ впервые "родился" в 1998 году и с тех пор "лежал на полке" практически без изменений. Чтобы проведенная работа не пропала впустую я решил выпустить свое детище в свет так, как оно есть, - без изменений и правок. Это первая версия, которая будет обновляться и изменяться в соответствии с вашими пожеланиями и рекомендациями.

Многие термины могут вызвать нарекания. Некоторых терминов пока в словаре нет, но это работа будет продолжаться и надеюсь, что совместными усилиями данный документ примет нужные очертания.

По всем вопросам, связанным с документом, прошу обращаться ко мне по адресам: luka@infosec.ru или firesnow@mail.ru.

ОГЛАВЛЕНИЕ

А	23
<hr/>	
АТАКА	23
АУТЕНТИФИКАЦИЯ	23
АУТЕНТИФИКАЦИЯ ОДНОСТОРОННЯЯ	23
АУТЕНТИФИКАЦИЯ ВЗАИМНАЯ	23
АУТЕНТИФИКАЦИЯ СЛАБАЯ	23
АУТЕНТИФИКАЦИЯ СИЛЬНАЯ	23
АВТОРИЗАЦИЯ	23
АВТОРИЗОВАННЫЙ СУБЪЕКТ ДОСТУПА	24
АТТЕСТАЦИЯ	24
АТТЕСТАЦИЯ ИСПЫТАТЕЛЬНЫХ ЛАБОРАТОРИЙ	24
АТТЕСТАЦИЯ ОБЪЕКТА В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ	24
АНАЛИЗ ЗАЩИЩЕННОСТИ	24
АНАЛИЗ РИСКА	25
АППАРАТНОЕ СРЕДСТВО ЗАЩИТЫ	25
АНТИВИРУСНАЯ ПРОГРАММА	25
АТРИБУТ ДОСТУПА	25
АУДИТ	25
АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОБРАБОТКИ ИНФОРМАЦИИ	25
АДМИНИСТРАТОР БЕЗОПАСНОСТИ	26
АДМИНИСТРАТИВНЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ	26
АППАРАТНО-ПРОГРАММНЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ	26
АБОНЕНТСКОЕ ШИФРОВАНИЕ	26
АККРЕДИТАЦИЯ	26
АНАЛИЗ ТРАФИКА	26
АГЕНТСТВО НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ	26
Б	27
<hr/>	
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ	27
БЕЗОПАСНОСТЬ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ	27
БЕЗОПАСНОСТЬ АС	27
БЕЗОПАСНОСТЬ РЕСУРСА АС	27
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ	27
БРАНДМАУЭР	28
БОМБА ЛОГИЧЕСКАЯ	28
БОМБА ВРЕМЕННАЯ	28
БЛОЧНЫЙ ШИФР	28
БЕЛЛА-ЛАПАДУЛЛА МОДЕЛЬ	28
БЬЮФОРТА КВАДРАТ	29
БЕССПОРНАЯ ПОДПИСЬ	29
БАСТИОН	29
В	30
<hr/>	
ВЕРИФИКАЦИЯ	30
ВЕРИФИКАТОР БАЙТ-КОДА	30

ВИРУС	30
ВОССТАНОВИТЕЛЬНЫЕ ПРОЦЕДУРЫ	30
ВИЖИНЕРА КВАДРАТ	30
ВЕРОЯТНОСТНОЕ ШИФРОВАНИЕ	30
ВЛАДЕЛЕЦ ИНФОРМАЦИИ	31

Г **32**

ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ ПРИ ПРЕЗИДЕНТЕ РФ	32
ГОСТЕХКОМИССИЯ РФ	32
ГТК РФ	32
ГОСТ 28147-89	32
ГОСТ Р 34.10-94	32
ГОСТ Р 34.11-94	33
ГОСТ Р 50739-95	33
ГОСТ Р 50922-96	33
Гриф	33
ГАММА ШИФРА	33
ГАММИРОВАНИЕ	34
ГАРАНТИИ	34
ГЕНЕРАТОР КЛЮЧЕВОГО ПОТОКА	34
ГРУППОВАЯ ПОДПИСЬ	34
ГЕНЕРАЦИЯ КЛЮЧЕЙ	34

Д **35**

ДОСТОВЕРНОСТЬ ИНФОРМАЦИИ	35
ДОСТУПНОСТЬ СИСТЕМЫ	35
ДОСТУП	35
ДОСТУП К РЕСУРСУ	35
ДИСКРЕЦИОННЫЙ ДОСТУП	35
ДИФФИ-ХЕЛЛМАНА АЛГОРИТМ	35
ДОСТОВЕРНАЯ ВЫЧИСЛИТЕЛЬНАЯ БАЗА	36
ДВБ	36
ДОМЕН	36
ДОСТОВЕРНЫЙ МАРШРУТ	36
ДЖЕФФЕРСОНА КОЛЕСО	36
ДОСКА ПОЛИБИЯ	37
ДЕКОДИРОВАНИЕ	37
ДЕРЕВО МЕРКЛЯ	37
ДИФФЕРЕНЦИАЛЬНЫЙ КРИПТОАНАЛИЗ	37
ДЕПОНИРОВАНИЕ КЛЮЧЕЙ	37
ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ	37

З **38**

ЗАЩИТА ИНФОРМАЦИИ	38
ЗАШИФРОВАНИЕ	38
ЗАЩИЩЕННОСТЬ	38
ЗОНА БЕЗОПАСНОСТИ	38
ЗЛОУМЫШЛЕННИК	38

И	39
ИДЕНТИФИКАЦИЯ	39
ИДЕНТИФИКАТОР	39
ИЗБИРАТЕЛЬНЫЙ ДОСТУП	39
ИНФОРМАЦИЯ	39
ИМИТОЗАЩИТА	39
ИМИТОВСТАВКА	40
ИНСТРУКТИВНЫЕ УКАЗАНИЯ ГОСУДАРСТВЕННОГО АРБИТРАЖА СССР № И-1-4	40
К	41
Ключ криптографический	41
Код	41
КОДИРОВАНИЕ	41
КРИПТОГРАФИЯ	41
КРИПТОГРАФИЧЕСКАЯ СИСТЕМА	41
КОНТРОЛЬ ДОСТУПА	41
КОНФИДЕНЦИАЛЬНОСТЬ	41
КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ	42
КОНЦЕПЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ	42
КРИПТОАНАЛИЗ	42
КРИПТОЛОГИЯ	42
КЛАСС ЗАЩИЩЕННОСТИ	43
КЛЮЧЕВАЯ СИСТЕМА	43
КАНАЛЬНОЕ ШИФРОВАНИЕ	43
КРАСНАЯ КНИГА	43
КОМПРОМЕТАЦИЯ ИНФОРМАЦИИ	43
КРИПТОСИСТЕМА С СЕКРЕТНЫМ КЛЮЧОМ	43
КРИПТОСИСТЕМА С ОТКРЫТЫМ КЛЮЧОМ	44
КВАДРАТ ВИЖИНЕРА	44
КАЗИСКИ МЕТОД	44
КВАДРАТ ПОЛИБИЯ	44
КАРДАНО РЕШЕТКА	44
Коды, исправляющие ошибки	45
Коды Гоппы	45
КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ	45
КРИПТОГРАФИЧЕСКОЕ ПРЕОБРАЗОВАНИЕ ИНФОРМАЦИИ	45
КВАНТОВАЯ КРИПТОГРАФИЯ	45
КРИПТОСИСТЕМА С ВРЕМЕННЫМ РАСКРЫТИЕМ	46
КРИПТОСИСТЕМА С ЭЛЛИПТИЧЕСКИМИ КРИВЫМИ	46
КРИПТОСИСТЕМА МАКЭЛИСА	46
КРИПТОСИСТЕМА НИДЕРРАЙТЕРА	46
КРИПТОСИСТЕМА ГАБИДУЛИНА	46
КРИПТОСИСТЕМА КРУКА	46
КРИПТОСИСТЕМА ВЕРНАМА	47
КОЛЛИЗИЯ	47
Код аутентификации сообщения	47
Код целостности сообщений	47
КОНТРОЛЬ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ	47
Л	48

ЛИЦЕНЗИРОВАНИЕ	48
ЛИЦЕНЗИЯ	48
ЛИЦЕНЗИАТ	48
ЛИЦЕНЗИАР	48
ЛЮК	48
ЛОГИЧЕСКАЯ БОМБА	48
ЛИНЕЙНЫЙ КРИПТОАНАЛИЗ	48

М **50**

МАНДАТНЫЙ ДОСТУП	50
МАСКАРАД	50
МОРАЛЬНО-ЭТИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ	50
МАТРИЦА ДОСТУПА	51
МАНДАТ	51
МИНИМУМ ПРИВИЛЕГИЙ	51
МНОГОУРОВНЕВАЯ БЕЗОПАСНОСТЬ	51
МОНИТОР ССЫЛОК	51
МЕТКА КОНФИДЕНЦИАЛЬНОСТИ	51
МНОГОУРОВНЕВАЯ ЗАЩИТА	51
МОДЕЛЬ НАРУШИТЕЛЯ	52
МОДЕЛЬ ЗАЩИТЫ	52
МНОГОУРОВНЕВАЯ КРИПТОГРАФИЯ	52

Н **53**

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП	53
НСД	53
НЕСАНКЦИОНИРОВАННОЕ ДЕЙСТВИЕ	53
НАРУШИТЕЛЬ	53
НАЦИОНАЛЬНЫЙ ЦЕНТР КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ	53
НОСИТЕЛИ ИНФОРМАЦИИ	53
НОРМЫ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ	54

О **55**

ОТКРЫТЫЙ КЛЮЧ	55
ОТКРЫТЫЙ ТЕКСТ	55
ОБНАРУЖЕНИЕ АТАК	55
ОБРАБОТКА ИНФОРМАЦИИ В АС	55
ОБЪЕКТ	55
ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ	55
ОТКАЗ В ОБСЛУЖИВАНИИ	56
ОРАНЖЕВАЯ КНИГА	56
ОКОНЕЧНОЕ ШИФРОВАНИЕ	56
ОДНОСТОРОННЯЯ ФУНКЦИЯ	56
ОДНОСТОРОННЯЯ ФУНКЦИЯ С СЕКРЕТОМ	56
ОТКРЫТОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ	56
ОДНОРАЗОВАЯ ЦИФРОВАЯ ПОДПИСЬ	57
ОДНОРАЗОВЫЙ БЛОКНОТ	57

П **58**

ПАРОЛЬ	58
ПОЛНОМОЧИЯ	58
ПРАВИЛО ДОСТУПА	58
ПРАВО ДОСТУПА	58
ПРОФИЛЬ ПОЛНОМОЧИЙ	58
ПРИВИЛЕГИИ	58
ПЛАН ЗАЩИТЫ	58
ПОЛИТИКА БЕЗОПАСНОСТИ	58
ПОДПИСЬ КОДА	59
ПОТОВОКОВЫЙ ШИФР	59
ПРАВИЛА РАЗГРАНИЧЕНИЯ ДОСТУПА	59
ПРАВОВЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ	59
ПОЛНОМОЧНЫЙ ДОСТУП	59
ПОДОТЧЕТНОСТЬ	60
ПЛАН ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОЙ РАБОТЫ И ВОССТАНОВЛЕНИЯ	60
ПОВТОРНОЕ ИСПОЛЬЗОВАНИЕ ОБЪЕКТА	60
ПРАВИЛО КИРКОФФА	60
ПОЛИБИЯ КВАДРАТ	60
ПОКАЗАТЕЛЬ ЗАЩИЩЕННОСТИ	60
ПРОТОКОЛ С АРБИТРОМ	60
ПРОТОКОЛ С ТРЕТЕЙСКИМ СУДЬЕЙ	61
ПРОТОКОЛ, САМООБЕСПЕЧИВАЮЩИЙ ЗАКОННОСТЬ	61
ПРОТОКОЛ ОТРИЦАНИЯ	61
ПОЛНЫЙ ПЕРЕБОР	61
ПОСРЕДНИК	61
ПОКАЗАТЕЛЬ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ	61
ПОЛЬЗОВАТЕЛЬ ИНФОРМАЦИИ	61
ПОТРЕБИТЕЛЬ ИНФОРМАЦИИ	62
ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ №1233	62
ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ №333	62
ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РСФСР №35	62
ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ №608	62
ПИСЬМО ВЫСШЕГО АРБИТРАЖНОГО СУДА РФ № С1-7/ОП-587	62
ПИСЬМО ВЫСШЕГО АРБИТРАЖНОГО СУДА РФ № С1-7/ОЗ-316	63
Р	64
РАЗГРАНИЧЕНИЕ ДОСТУПА	64
РАСШИФРОВАНИЕ	64
РАСПОЗНАВАНИЕ АТАКИ	64
РЕГЛАМЕНТАЦИЯ	64
РУКОВОДЯЩИЙ ДОКУМЕНТ	64
РАДУЖНАЯ СЕРИЯ	64
РОТОРНАЯ МАШИНА	65
РЕШЕТКА КАРДАНО	65
РАЗДЕЛЕНИЕ СЕКРЕТОВ	65
РЕГИСТР СДВИГА С ОБРАТНОЙ СВЯЗЬЮ	65
РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ	65
РЕШЕНИЕ ГОСТЕХКОМИССИИ И ФАПСИ №10	65
РУКОВОДЯЩИЙ ДОКУМЕНТ «КОНЦЕПЦИЯ ЗАЩИТЫ СВТ И АС ОТ НСД К ИНФОРМАЦИИ»	66
РУКОВОДЯЩИЙ ДОКУМЕНТ «ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ»	66
РУКОВОДЯЩИЙ ДОКУМЕНТ «ВРЕМЕННОЕ ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ РАЗРАБОТКИ, ИЗГОТОВЛЕНИЯ И ЭКСПЛУАТАЦИИ ПРОГРАММНЫХ И ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ	

ИНФОРМАЦИИ ОТ НСД В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ И СРЕДСТВАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ»	66
Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»	67
Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации»	67
Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»	67
Руководящий документ «Защита информации. Специальные защитные знаки. Классификация и общие требования»	68
С	69
Сертификация СЗИ	69
Сертификат соответствия	69
Система защиты информации	69
Система криптографической защиты информации	69
Система обнаружения атак	69
Система анализа защищенности	70
СКРЕМБЛЕР	70
Средство защиты информации	70
Стойкость	70
СНИФФИНГ	70
СПУФФИНГ	70
СУБЪЕКТЫ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ	70
СУБЪЕКТ	71
«САЛЯМИ» АТАКА	71
СКРЫТЫЕ КАНАЛЫ	71
СКРЫТЫЙ ВРЕМЕННОЙ КАНАЛ	71
СКРЫТЫЙ КАНАЛ С ПАМЯТЬЮ	71
СБОРКА МУСОРА	71
СПИСОК КОНТРОЛЯ ДОСТУПА	71
СТОРНЕТТА-ХАБЕРА АЛГОРИТМ	71
СТЕГАНОГРАФИЯ	72
СИНХРОНИЗИРУЮЩАЯ ПОТОКОВАЯ КРИПТОСИСТЕМА	72
САМОСИНХРОНИЗИРУЮЩАЯ ПОТОКОВАЯ КРИПТОСИСТЕМА	72
СЧЕТЧИКОВЫЙ МЕТОД	72
СОВЕРШЕННАЯ СЕКРЕТНОСТЬ	73
СЛЕПАЯ ПОДПИСЬ	73
САМОПРОВЕРЯЮЩАЯСЯ ПОДПИСЬ	73
СЕРТИФИКАТ КЛЮЧА	73
СПИСОК АННУЛИРОВАННЫХ СЕРТИФИКАТОВ	73
СЕРВЕР-ПОСРЕДНИК	73
СЕКРЕТНЫЙ КЛЮЧ	73
СОБСТВЕННИК ИНФОРМАЦИИ	74
Т	75
Троянский конь	75
Технические меры защиты информации	75

ТУННЕЛИРОВАНИЕ	75
У	76
Уязвимость АС	76
Уязвимость субъекта информационных отношений	76
Уязвимость информации	76
Угроза АС	76
Угроза интересам субъектов информационных отношений	76
Угроза безопасности информации	76
Управление ключами	77
Управление доступом	77
Уровень безопасности	77
Уровень прозрачности	77
Уровень доступа	77
Уровень полномочий	77
Уровень привилегий	77
Установление подлинности	77
Указ Президента РФ №334	77
Указ Президента РФ №188	78
Ф	79
Федеральное агентство правительственной связи и информации	79
ФАПСИ	79
Физические меры защиты информации	79
Х	80
Хэш-функция	80
ХАГЕЛИНА МАШИНА	80
Ц	81
Целостность	81
Цифровая подпись	81
Цель защиты информации	81
Центр распределения ключей	81
Центр сертификации ключей	81
Цифровой конверт	82
Ч	83
Червь	83
Ш	84
Шифр	84
Шифрование	84
Шифртекст	84

ШАРАДЫ МЕРКЛЯ	84
ШАРАДЫ С ВРЕМЕННЫМ ЗАМКОМ	84
ШИФР ФЕЙСТЕЛЯ	85
ШЛЮЗ ПРИКЛАДНОГО УРОВНЯ	85
ШЛЮЗ СЕАНСОВОГО УРОВНЯ	85
ШЛЮЗ ДВУХПОРТОВЫЙ	85
ШИФРОВАЛЬНЫЕ СРЕДСТВА	85
Э	86
<hr/>	
ЭКРАН МЕЖСЕТЕВОЙ	86
ЭКРАН МЕЖСЕТЕВОЙ С ФИЛЬТРАЦИЕЙ ПАКЕТОВ	86
ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ	86
ЭЦП	86
ЭКСПОНЕНЦИАЛЬНОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ	87
ЭЛЬ-ГАМАЛЯ АЛГОРИТМ	87
ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ	87
ЭФФЕКТИВНОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ	87
Я	88
<hr/>	
ЯДРО БЕЗОПАСНОСТИ	88
А	89
<hr/>	
AMERICAN NATIONAL STANDARDS INSTITUTE	89
ANSI	89
ANSI X9.9	89
ANSI X9.17	89
ANSI X9.23	89
ANSI X9.30	89
ANSI X9.31	89
ANSI X9.41	90
ANSI X9.42	90
ANSI X9.44	90
ANSI X9.45	90
ANSI X12.58	90
AUTHENTICODE	90
ASSIST	90
AUTOMATED SYSTEMS SECURITY INCIDENT SUPPORT TEAM	91
AUDIT	91
AUDIT TRAIL	91
AUTHENTICATION	91
ACCESS PERIOD	91
ACCESS CONTROL	91
ACCESS CONTROL LIST	91
СМ. СБОРКА МУСОРА	91
ACCOUNTABILITY	91
ASSURANCE	92
AUTHORIZATION	92
ASYMMETRIC CRYPTOGRAPHY	92
ADAPTIVE CHOSEN CIPHERTEXT ATTACK	92
ARBITRATED PROTOCOL	92

ADJUDICATED PROTOCOL	92
AS2805.6.5.3	92
APPLICATION-LEVEL GATEWAY	92
A GUIDE TO UNDERSTANDING AUDIT IN TRUSTED SYSTEMS	93
A GUIDE TO UNDERSTANDING DISCRETIONARY ACCESS CONTROL IN TRUSTED SYSTEMS	93
A GUIDE TO UNDERSTANDING CONFIGURATION MANAGEMENT IN TRUSTED SYSTEMS	93
A GUIDE TO UNDERSTANDING DESIGN DOCUMENTATION IN TRUSTED SYSTEMS	93
A GUIDE TO UNDERSTANDING TRUSTED DISTRIBUTION IN TRUSTED SYSTEMS	94
A GUIDE TO UNDERSTANDING SECURITY MODELING IN TRUSTED SYSTEMS	94
A GUIDE TO UNDERSTANDING TRUSTED FACILITY MANUALS	94
A GUIDE TO UNDERSTANDING IDENTIFICATION AND AUTHENTICATION IN TRUSTED SYSTEMS	94
A GUIDE TO UNDERSTANDING OBJECT REUSE IN TRUSTED SYSTEMS	95
A GUIDE TO UNDERSTANDING TRUSTED RECOVERY IN TRUSTED SYSTEMS	95
A GUIDE TO UNDERSTANDING SECURITY TESTING AND TEST DOCUMENTATION IN TRUSTED SYSTEMS	95
A GUIDE TO PROCUREMENT OF TRUSTED SYSTEMS: AN INTRODUCTION TO PROCUREMENT INITIATORS ON COMPUTER SECURITY REQUIREMENTS	95
A GUIDE TO PROCUREMENT OF TRUSTED SYSTEMS: LANGUAGE FOR RFP SPECIFICATIONS AND STATEMENTS OF WORK – AN AID TO PROCUREMENT INITIATORS	95
A GUIDE TO PROCUREMENT OF TRUSTED SYSTEMS: COMPUTER SECURITY CONTRACT DATA REQUIREMENTS LIST AND DATA ITEM DESCRIPTION TUTORIAL	96
A GUIDE TO PROCUREMENT OF TRUSTED SYSTEMS: HOW TO EVALUATE A BIDDER'S PROPOSAL DOCUMENT – AN AID TO PROCUREMENT INITIATORS AND CONTRACTORS	96
A GUIDE TO UNDERSTANDING DATA REMANENCE IN AUTOMATED INFORMATION SYSTEMS	96
A GUIDE TO WRITING THE SECURITY FEATURES USER'S GUIDE FOR TRUSTED SYSTEMS	97
A GUIDE TO UNDERSTANDING INFORMATION SYSTEM SECURITY OFFICER RESPONSIBILITIES FOR AUTOMATED INFORMATION SYSTEMS	97
ACCESSING CONTROLLED ACCESS PROTECTION	97
A GUIDE TO UNDERSTANDING COVERT CHANNEL ANALYSIS OF TRUSTED SYSTEMS	97
AES	97
ADVANCED ENCRYPTION STANDARD	98
AMBER BOOK	98
AQUA BOOK	98
B	99
BLOWFISH	99
BLOCK CIPHER	99
BELL-LAPADULLA MODEL	99
BACKUP PLAN	99
BANKING CIRCULAR 226	99
BC-226	99
BANKING CIRCULAR 229	99
BC-229	99
BLIND SIGNATURE SCHEME	100
BRUTE-FORCE ATTACK	100
BRUTE-FORCE SEARCH	100
BIRTHDAY ATTACK	100
BASTION HOST	101
BRIGHT BLUE BOOK	101
BURGUNDY BOOK	101
BROWN BOOK	101
BLUE BOOK	101
BRIGHT ORANGE BOOK	101

C	102
CIPHER	102
CIPHERTEXT	102
CIPHER BLOCK CHAINING	102
CBC	102
CIPHER FEEDBACK	102
CFB	102
CAPSTONE	103
CLIPPER	103
CODE SIGNING	103
CERT	103
COMPUTER EMERGENCY RESPONSE TEAM	103
CIAC	104
COMPUTER INCIDENT ADVISORY CAPABILITY	104
CRYPTOGRAPHY	104
COVERT CHANNELS	104
COVERT STORAGE CHANNEL	105
COVERT TIMING CHANNEL	105
CAPABILITY	105
CONFIDENTIALITY	105
CONTINGENCY PLAN	105
COMPUTER SECURITY AGENCY	105
COMMERCIAL PRODUCT EVALUATION	105
COMMERCIAL COMPUTER SECURITY CENTRE	106
COMPROMISE	106
COUNTERFEIT ACCESS DEVICE AND COMPUTER FRAUD AND ABUSE ACT OF 1984	106
COMPUTER FRAUD AND ABUSE ACT OF 1986	106
COMPUTER SECURITY ACT OF 1987, PL 100-235	106
COMPUTER MISUSE ACT OF 1990	106
CHOSEN PLAINTEXT ATTACK	106
CHOSEN CIPHERTEXT ATTACK	107
CHOSEN MESSAGE ATTACK	107
CIPHERTEXT ONLY ATTACK	107
CHOSEN KEY ATTACK	107
C-36	107
COUNTER METHOD	107
CIPHERTEXT AUTO KEY	107
CTAK	108
CERTIFICATE	108
CERTIFICATE REVOCATION LIST	108
CAPI	108
CRYPTOGRAPHIC APPLICATION PROGRAMMING INTERFACE	108
CRYPTOKI	108
CIRCUIT-LEVEL GATEWAY	108
CHALLENGE-HANDSHAKE AUTHENTICATION PROTOCOL	108
CHAP	109
COMPUTER OPERATIONS AUDIT AND SECURITY TECHNOLOGY	109
COAST	109
COMPUTER SECURITY REQUIREMENTS – GUIDANCE FOR APPLYING THE DoD TCSEC IN SPECIFIC ENVIRONMENTS	109
COMPUTER SECURITY SUBSYSTEM INTERPRETATION OF THE TCSEC	109
CSC-STD-001-83	109
CSC-STD-002-85	110
CSC-STD-003-85	110

CSC-STD-004-85	110
D	111
DIGITAL SIGNATURE ALGORITHM	111
DSA	111
DIGITAL SIGNATURE STANDARD	111
DSS	111
DIFFIE-HELLMAN	111
DATA ENCRYPTION STANDARD	111
DES	111
DESX	112
CM. ТАКЖЕ DATA ENCRYPTION STANDARD	112
DISK SCAVENGING	112
DENIAL OF SERVICE	112
DISCRETIONARY ACCESS CONTROL	112
DEPARTMENT OF DEFENSE	112
DoD	112
DoD GUIDELINES FOR COMPUTER SECURITY	112
DOMAIN	113
DAC	113
DATA SECURITY OFFICER	113
DSO	113
DATA COMPUTER ACT OF 1984	113
DESIGNATED CONFIRMER SIGNATURE	113
DIFFERENTIAL CRYPTANALYSIS	113
DES-EEE3	113
DES-EDE3	114
DES-EEE2	114
DES-EDE2	114
DIGITAL FINGERPRINT	114
DAVIES-MEYER HASH FUNCTION	114
DUAL-HOMED GATEWAY	114
DEMILITARIZED ZONE	114
DMZ	115
DIGITAL ENVELOP	115
DARK LAVENDER BOOK	115
E	116
ELGAMAL	116
ELLIPTIC CURVES	116
ELECTRONIC CODEBOOK	116
ECB	116
EVALUATED PRODUCTS LIST	116
EPL	116
ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986	117
ENIGMA	117
E31.20	117
ETEBAC 5	117
EXPONENTIAL KEY AGREEMENT	117
EXHAUSTIVE KEY SEARCH	117
ESCROWED ENCRYPTION STANDARD	117

EES	117
F	118
FORTEZZA	118
FEAL	118
FAST DATA ENCIPHERMENT ALGORITHM	118
FLAW	118
FAULT	118
FOREIGN CORRUPT PRACTICES ACT OF 1977	118
FAPKC	118
FAIL-STOP SIGNATURE SCHEME	119
FIREWALL	119
FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS	119
FIRST	119
FEDERAL COMPUTER INCIDENT RESPONSE CAPABILITY	120
FEDCIRC	120
FOREST GREEN BOOK	120
G	121
G-DES	121
GARBAGE COLLECTING	121
GREEDY PROGRAM	121
GREEN BOOK	121
GUESSED PLAINTEXT ATTACK	121
GROUP SIGNATURE	121
GLOSSARY OF COMPUTER SECURITY TERMS	122
GUIDELINES FOR FORMAL VERIFICATION SYSTEMS	122
GUIDELINES FOR WRITING TRUSTED FACILITY MANUALS	122
H	123
HASH	123
HOLE	123
HOT PEACH BOOK	123
I	124
IKP	124
INTERNET KEYED PAYMENTS PROTOCOL	124
INTERNATIONAL ORGANIZATION FOR STANDARDIZATION	124
ISO	124
IEEE P1363	124
IEEE 802.10C	124
IDEA	124
INTERNATIONAL DATA ENCRYPTION ALGORITHM	125
IP-SPOOFING	125
IDENTIFICATION	125
INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA	125
ITSEC	125
INTERNAL FEEDBACK	125

ITERATED BLOCK CIPHER	126
INTRUSION	126
INTRUSION DETECTION	126
INTRUSION DETECTION SYSTEM	126
IPSEC	126
IP SECURITY PROTOCOL	126
CM. ТАКЖЕ INTERNET SECURITY ASSOCIATION & KEY MANAGEMENT PROTOCOL	127
ISAKMP	ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.
INTEGRITY	127
INTRODUCTION TO CERTIFICATION AND ACCREDITATION CONCEPTS	127
INTERNET SECURITY ASSOCIATION & KEY MANAGEMENT PROTOCOL	127
ISAKMP	127
IKE	127
INTERNET KEY EXCHANGE	127

K **129**

KNAPSACK	129
KERBEROS	129
KNOWN PLAINTEXT ATTACK	129
KEY	129
KEY STREAM GENERATOR	129
KEY AUTO KEY	129
КАК	129
KEY SCHEDULE	129
KEY MANAGEMENT	130
KEY GENERATION	130
KEY DISTRIBUTION	130
KEY STORAGE	130
KEY DELETION	130
KEY RECOVERY	130
KEY CRUNCHING	130
KEY ESCROW	130

L **132**

LUC	132
LEAST PRIVILEGE	132
LINK ENCRYPTION	132
LOOPHOLE	132
LABEL	132
LINEAR FEEDBACK SHIFT REGISTER	132
LFSR	132
LAYER 2 FORWARDING	132
L2F	133
LAYER 2 TUNNELING PROTOCOL	133
L2TP	133
LIGHT YELLOW BOOK	133
LIGHT BLUE BOOK	133
LIGHT PINK BOOK	133

M **134**

MERKLE'S TREE	134
MCELIECE CRYPTOSYSTEM	134
MIME OBJECT SECURITY SERVICE	134
MOSS	134
MAC	134
MD2	134
MD4	135
MD5	135
MASQUERADE	135
MANDATORY ACCESS CONTROL	135
MULTILEVEL SECURITY	135
M-209 CONVERTER	135
MESSAGE AUTHENTICATION CODE	135
MESSAGE INTEGRITY CHECK	136
MESSAGE SECURITY PROTOCOL	136
MSP	136
MAN-IN-THE-MIDDLE	136
MIDDLEPERSON ATTACK	136
MESSAGE DIGEST	136
N	137
<hr/>	
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY	137
NIST	137
NBS	137
NATIONAL SECURITY AGENCY	137
NSA	137
NASIRC	137
NASA AUTOMATED SYSTEMS INCIDENT RESPONSE CAPABILITY	137
NATIONAL COMPUTER SECURITY CENTER	138
NCSC	138
NONREPUDIATION	138
NEW DIRECTIONS IN CRYPTOGRAPHY	138
NIEDERREITER CRYPTOSYSTEM	138
NCSC-TG-001	138
NCSC-TG-002	138
NCSC-TG-003	139
NCSC-TG-004	139
NCSC-TG-005	139
NCSC-TG-006	139
NCSC-TG-007	139
NCSC-TG-008	139
NCSC-TG-009	139
NCSC-TG-010	139
NCSC-TG-011	139
NCSC-TG-013	139
NCSC-TG-014	139
NCSC-TG-015	140
NCSC-TG-016	140
NCSC-TG-017	140
NCSC-TG-018	140
NCSC-TG-019	140
NCSC-TG-020	140
NCSC-TG-021	140

NCSC-TG-022	140
NCSC-TG-023	140
NCSC-TG-024	140
NCSC-TG-025	140
NCSC-TG-026	141
NCSC-TG-027	141
NCSC-TG-028	141
NCSC-TG-029	141
NCSC-TG-030	141
NEON ORANGE BOOK	141

O 142

ONE-TIME PAD	142
OUTPUT FEEDBACK	142
OFB	142
OBJECT SIGNING	142
ORANGE BOOK	142
OBJECT	142
OBJECT REUSE	142
OMBA-123	143
OPUS NOVUM	143
ONE-WAY FUNCTION	143
ONE-TIME SIGNATURE	143
OAKLEY	143

P 144

PKCS	144
PKCS #1	144
PKCS #3	144
PKCS #5	144
PKCS #6	144
PKCS #7	144
PKCS #8	144
PKCS #9	144
PKCS #10	145
PKCS #11	145
PUBLIC-KEY CRYPTOGRAPHY STANDARDS	145
PUBLIC KEY	145
PRIVATE KEY	145
PRIVACY ENHANCED MAIL	145
PEM	146
PEM-MIME	146
PCT	146
PRIVATE COMMUNICATION TECHNOLOGY	146
POINT-TO-POINT TUNNELING PROTOCOL	146
PPTP	146
PRINCIPAL	146
PREFERRED PRODUCTS LIST	147
PPL	147
PROCESS	147
PROTOCOL	147

PLAINTEXT	147
PUBLIC-KEY CRYPTOGRAPHY	147
PRIVACY ACT OF 1974	147
PURCHASE KEY ATTACK	147
PURPLE	147
POLYGRAPHIA	148
PROPAGATING CIPHER BLOCK CHAINING	148
PCBC	148
PLAINTEXT BLOCK CHAINING	148
PBC	148
PACKET-FILTERING FIREWALL	148
PROXY	148
PROXY SERVER	149
PASSWORD AUTHENTICATION PROTOCOL	149
PAP	149
PERSONAL INFORMATION EXCHANGE	149
PFX	149
PARTIAL KEY ESCROW	149
PASSWORD MANAGEMENT GUIDELINE	150
PINK BOOK	150
PURPLE BOOK	150
Q	151
<hr/>	
QUANTUM CRYPTOGRAPHY	151
R	152
<hr/>	
RSA	152
RC2	152
RC4	153
RC5	153
RISK ANALYSIS	153
RAINBOW SERIES	153
RECOVERY PLAN	153
RECOVERY PROCEDURES	153
REFERENCE MONITOR CONCEPT	153
REPUDIATION	153
RUBBER HOSE CRYPTANALYSIS	154
RED	154
RUNNING KEY GENERATOR	154
RABIN SIGNATURE SCHEME	154
RSA-129	154
RDES	154
RADIUS	155
REMOTE AUTHENTICATION DIAL-IN USER SERVICE	155
REMANENCE	155
RAMP PROGRAM DOCUMENT	155
RED BOOK	155
S	156
<hr/>	
SET	156

SECURE ELECTRONIC TRANSACTION	156
SSL	156
SECURE SOCKETS LAYER	156
S/WAN	156
SECURE WIDE AREA NETWORK	156
S\MIME	157
STREAM CIPHER	157
SKIPJACK	157
S1	157
SEAL	157
SOFTWARE-OPTIMIZED ENCRYPTION ALGORITHM	157
SCREENING EXTERNAL ACCESS LINK	158
SAFER	158
SECURE AND FAST ENCRYPTION ROUTINE	158
SHA	158
SHS	158
SECURE HYPERTEXT TRANSFER PROTOCOL	159
S-HTTP	159
SIMPLE KEY MANAGEMENT FOR INTERNET PROTOCOL	159
SKIP	159
SNIFFING	159
SPOOFING	160
SALAMI ATTACK	160
SECURITY POLICY	160
SECURITY CLEARANCE	160
SUBJECT	160
SECURE STATE	160
SECURITY FLAW	161
SECURITY HOLE	161
SECURITY KERNEL	161
SECURITY LEVEL	161
SECRET-KEY CRYPTOGRAPHY	161
SYMMETRIC CRYPTOGRAPHY	161
SIGABA	161
SUBTILITAS DE SUBTILITAE RERUM	161
SYNCHRONOUS STREAM CIPHER	161
SELF SYNCHRONOUS STREAM CIPHER	162
SELF ENFORCING PROTOCOL	162
SELF-AUTHENTICATING SIGNATURE SCHEME	162
S ⁿ DES	162
SECRET SHARING SCHEME	162
SHAMIR'S SECRET SHARING SCHEME	162
SECURE COURIER	162
SECURITY ZONE	162
STATEFUL INSPECTION FIREWALL	163
SECURITY COORDINATION CENTER	163
SCC	163
SILVER BOOK	163
T	164
TRIPLE DES	164
TRAPDOOR	164
TROJAN HORSE	164

TRUSTED COMPUTING BASE	164
TCB	164
TEMPEST	164
THREAT	164
TRUSTED PATH	164
TRUSTED COMPUTER SECURITY EVALUATION CRITERIA	165
TCSEC	165
THE TRUSTED NETWORK INTERPRETATION OF DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION GUIDELINES	165
TIMESTAMPING	166
TIMED-RELEASE CRYPTOSYSTEM	166
TIMELOCK PUZZLES	166
TECHNICAL CRITERIA FOR EVALUATION OF COMMERCIAL SECURITY PRODUCTS	166
TRAP DOOR ONE-WAY FUNCTION	166
TESSERA	166
TERMINAL ACCESS CONTROL ACCESS SYSTEM	166
TACACS	167
TACACS+	167
TRANSPORT LAYER SECURE PROTOCOL	167
TLSP	167
TRAFFIC ANALYSIS	167
TECHNICAL RATIONAL BEHIND CSC-STD-003-85: COMPUTER SECURITY REQUIREMENTS – GUIDANCE FOR APPLYING THE DoD TCSEC IN SPECIFIC ENVIRONMENTS	167
TRUSTED PRODUCT EVALUATIONS – A GUIDE FOR VENDORS	168
TRUSTED PRODUCT EVALUATION PROGRAM	168
TPEP	168
TNI	168
TRUSTED NETWORK ENVIRONMENTS GUIDELINE – GUIDANCE FOR APPLYING THE TNI	168
TRUSTED PRODUCT EVALUATION QUESTIONNAIRE	168
TRUSTED UNIX WORKING GROUP (TRUSIX) RATIONALE FOR SELECTING ACCESS CONTROL	169
LIST FEATURES FOR THE UNIX® SYSTEM	169
TRUSTED DATABASE MANAGEMENT SYSTEM INTERPRETATION OF THE TCSEC	169
TDI	169
TAN BOOK	169
TEAL GREEN BOOK	169
TURQUOISE BOOK	169
U	170
<hr/>	
UNAUTHORIZED ACCESS	170
UNDENIABLE SIGNATURE SCHEME	170
V	171
<hr/>	
VERIFICATION	171
VULNERABILITY	171
VIOLATOR	171
VIRTUAL PRIVATE NETWORK	171
VPN	171
VENICE BLUE BOOK	171
VIOLET BOOK	171
W	172
<hr/>	

WORM	172
WHITE BOOK	172
WHITENING	172
X	173
<hr/>	
X.400	173
X.435	173
X.509	173
EXTENDED TERMINAL ACCESS CONTROL ACCESS SYSTEM	173
XTACACS	173
X-FORCE	173
Y	175
<hr/>	
YELLOW BOOK	175
YELLOW-GREEN BOOK	175
5	176
<hr/>	
5200.28-STD	176
СПИСОК ЛИТЕРАТУРЫ	177
<hr/>	
УКАЗАТЕЛЬ	178
<hr/>	

А

Атака

Действие нарушителя, которое приводит к реализации угрозы путем использования уязвимостей автоматизированной системы.

См. также Уязвимость АС, Угроза АС, Нарушитель.

Аутентификация

1. Проверка идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед выдачей разрешения на доступ).

См. также Идентификация, Доступ.

2. Проверка целостности данных при их хранении или передаче для предотвращения несанкционированной модификации.

См. также Электронная цифровая подпись, Хэш-функция, Целостность.

Аутентификация односторонняя

Аутентификация отправителя или получателя сообщения.

См. также Аутентификация, Аутентификация взаимная.

Аутентификация взаимная

Аутентификация, как отправителя, так и получателя сообщения.

См. также Аутентификация, Аутентификация односторонняя.

Аутентификация слабая

Проверка только идентификатора и пароля пользователя, инициирующего процесс аутентификации.

См. также Аутентификация, Аутентификация сильная.

Аутентификация сильная

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

См. также Аутентификация, Аутентификация слабая.

Авторизация

Предоставление субъекту прав на доступ к объекту.

См. также Доступ, Право доступа, Субъект.

Авторизованный субъект доступа

Субъект, которому предоставлены соответствующие права доступа (полномочия) к объектам системы.

См. также Авторизация.

Аттестация

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.

См. также Руководящий документ, Сертификация, Уровень безопасности.

Аттестация испытательных лабораторий

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

См. также Аттестация.

Аттестация объекта в защищенном исполнении

Официальное подтверждение наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований руководящих документов и норм эффективности защиты информации.

См. также Аттестация.

Анализ защищенности

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

См. также Уязвимость АС.

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

См. также Показатель эффективности защиты информации.

Анализ риска

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.

См. также Угроза безопасности информации.

Аппаратное средство защиты

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.

См. также Организационные меры защиты информации, Технические меры защиты информации, Несанкционированный доступ.

Антивирусная программа

Программа, обнаруживающая и/или удаляющая вирусы.

См. также Вирус.

Атрибут доступа

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”, “выполнение”).

См. также Доступ, Право доступа, Объект.

Аудит

1. Процесс получения и анализа записей системного журнала с целью установления текущего состояния защищенности системы.
2. Экспертиза автоматизированной системы и всех ее составляющих с целью определения состояния безопасности системы, ее соответствия требованиям действующего законодательства и организационно-распорядительных документов организации.

См. также Анализ защищенности, Анализ риска.

Автоматизированная система обработки информации

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.

Администратор безопасности

Лицо или группа лиц, ответственных за обеспечение безопасности системы, за реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляющих постоянную организационную поддержку функционирования применяемых физических и технических средств защиты.

Административные меры защиты информации

См. Организационные меры защиты информации

Аппаратно-программные меры защиты информации

См. Технические меры защиты

Абонентское шифрование

Криптографическая защита информации, передаваемой между двумя субъектами автоматизированной системы.

См. также Шифрование, Канальное шифрование.

Аккредитация

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 Госстанкомиссия РФ.

См. также Государственная техническая комиссия при Президенте РФ.

Анализ трафика

См. Sniffing

Агентство национальной безопасности

См. National Security Agency

Б

Безопасность информации

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.

Безопасность субъектов информационных отношений

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

Безопасность АС

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

Безопасность ресурса АС

Безопасность ресурса АС 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).

См. также Доступность, Конфиденциальность, Целостность.

Безопасность информационной технологии

Защищенность технологического процесса переработки информации.

Брандмауэр

Синоним (переводимый с немецкого языка как "Огненная стена") термина "Межсетевой экран" или "firewall", используемый в российских средствах массовой информации.

См. также Экран межсетевой.

Бомба логическая

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

См. также Бомба временная.

Бомба временная

Разновидность логической бомбы, выполняющейся в заданное время.

См. также Бомба логическая.

Блочный шифр

Преобразование блоков фиксированной длины открытого текста в блоки зашифрованного текста такой же длины независимо от положения блока во входной последовательности. Недостатком блочных шифров является искажение открытого текста вследствие распространения ошибок, возникающих в процессе передачи сообщения по каналу связи. К блочным криптосистемам можно отнести ГОСТ 28147-89 (режим простой замены), DES (режим ECB) и некоторые другие.

Во многих криптосистемах длина обрабатываемого блока равна 64 бит.

См. также Поточковый шифр, ГОСТ 28147-89, Data Encryption Standard.

Белла-Лападулла модель

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 безопасное), то согласно принципу индукции система является безопасной.

Состояние системы считается безопасным, если в соответствии с политикой безопасности субъектам разрешены только определенные типы доступа к объектам (в том числе отсутствие доступа). Для определения, разрешен субъекту доступ к объекту или нет, его уровень прозрачности сравнивается с меткой объекта (уровнем безопасности объекта) и для запрашиваемого типа доступа принимается решение - разрешить доступ или нет. Принятие решения осуществляется на основе двух правил: простого условия безопасности (simple security condition) и *-свойства (*-property или star property). Простое условие безопасности разрешает доступ, если уровень прозрачности субъекта не ниже метки критичности объекта. *-условие разрешает доступ, если:

- для чтения или выполнения - текущий уровень субъекта не ниже метки критичности объекта;
- для записи или модификации - текущий уровень субъекта не выше метки критичности объекта.

См. также Мандатный доступ.

Бьюфорта квадрат

Многоалфавитная криптосистема, аналогичная криптосистеме Вижинера. Строками квадрата являются строки квадрата Вижинера, записанные в обратном порядке. Криптосистема названа в честь адмирала Френсиса Бьюфорта.

См. также Криптографическая система.

Беспорная подпись

Схема цифровой подписи, предложенная в 1990 году Чомом (David Chaum) и Ван Антверпеном (van Antwerpen). В схемах, в которых подлинность сообщения проверяется только при помощи подписывающего лица, возможен отказ подписывающего от своего сообщения. Схема беспорной подписи использует протокол отрицания, который позволяет решить эту проблему.

См. также Протокол отрицания, Самопроверяющаяся подпись, Электронная цифровая подпись.

Бастيون

См. Bastion Host

В

Верификация

Процесс сопоставления двух уровней спецификаций системы (например, модели 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.

Верификатор байт-кода

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

Вирус

Компьютерная программа, способная «размножаться», «заражать» программы и файлы, модифицируя их так, чтобы они включали в себя копию вируса или его разновидность.

См. также Антивирусная программа, Червь.

Восстановительные процедуры

См. Recovery procedures

Вижинера квадрат

Одна из наиболее известных многоалфавитных криптосистем. Названа в честь французского криптографа Блейза Вижинера. 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.

См. также Бьюфорта квадрат, Казиски метод, Криптографическая система.

Вероятностное шифрование

Схема шифрования, предложенная Гольдвассером (Goldwasser) и Микали (Micali). В отличие от классических криптосистем, в которых каждому открытому тексту соответствует один шифртекст, в схеме вероятностного шифрования одному открытому тексту может соответствовать множество шифртекстов.

См. также Криптографическая система.

Владелец информации

1. Субъект, осуществляющий владение и пользование информацией и реализующий полномочия и распоряжения в пределах прав, установленных законом и/или собственником информации.
 2. Субъект информационных отношений, обладающий правом владения, распоряжения и пользования информационным ресурсом по договору с собственником информации.
- См. также Собственник информации, Пользователь информации.

Г

Государственная техническая комиссия при Президенте РФ

Государственная российская организация, созданная в соответствии с Указом Президента РФ от 5 января 1992 г. №9 в целях проведения единой технической политики и координации работ в области защиты информации. Возглавляет Государственную систему защиты информации от технических разведок. Является коллегиальным органом, в состав которого входят министры, председатели госкомитетов и их первые заместители.

Является главным в России органом по лицензированию деятельности в области защиты информации и сертификации средств защиты информации по требованиям безопасности информации. Гостехкомиссия РФ выпустила несколько руководящих документов, определяющих требования по защите информации.

См. также Руководящий документ, Федеральное агентство правительственной связи и информации, Аттестация, Аккредитация, Лицензирование, Сертификация СЗИ.

Гостехкомиссия РФ

См. Государственная техническая комиссия при Президенте РФ

ГТК РФ

См. Государственная техническая комиссия при Президенте РФ

ГОСТ 28147-89

Данный стандарт, введенный в действие 1 июля 1990 года, устанавливает единый алгоритм криптографического преобразования (шифрования) для отдельных компьютеров и вычислительных сетей. Полное наименование – «ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

Относится к разряду блочных шифров. Длина блока – 64 бита, а длина ключа – 256 бит. В стандарте предусмотрено 4 режима функционирования:

- зашифрование (расшифрование) данных в режиме простой замены;
- зашифрование (расшифрование) данных в режиме гаммирования;
- зашифрование (расшифрование) данных в режиме гаммирования с обратной связью;
- режим выработки имитовставки.

См. также Data Encryption Standard, Блочный шифр, Криптографическое преобразование, Гаммирование, Имитовставка.

ГОСТ Р 34.10-94

Данный стандарт, введенный в действие 1 января 1995 года, устанавливает процедуры выработки и проверки электронной цифровой подписи. Полное наименование – «ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».

Является модернизированным вариантом алгоритма ЭЦП с открытыми ключами Эль-Гамала. Длина ЭЦП – 512 бит.

См. также Эль-Гамала алгоритм, Электронная цифровая подпись.

ГОСТ Р 34.11-94

Данный стандарт, введенный в действие 1 января 1995 года, определяет алгоритм и процедуру вычисления хэш-функции для любой последовательности двоичных символов, которые применяются в криптографических методах обработки и защиты информации, в том числе для реализации процедур электронной цифровой подписи. Полное наименование – «ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования».

Длина хэш-функции – 256 бит.

См. также ГОСТ Р 34.10-94, Хэш-функция.

ГОСТ Р 50739-95

Данный стандарт, введенный в действие 1 января 1996 года, устанавливает единые функциональные требования к защите средств вычислительной техники (СВТ) от несанкционированного доступа (НСД) к информации, к составу документации на эти средства, а также номенклатуру показателей защищенности СВТ, описываемых совокупностью требований к защите и определяющих классификацию СВТ по уровню защищенности от НСД к информации.

Полное наименование - «ГОСТ Р 50739-95. Средства вычислительной техники. Защита информации от несанкционированного доступа к информации. Общие технические требования».

ГОСТ Р 50922-96

Данный стандарт, введенный в действие в 1996 году, устанавливает основные термины и их определения в области защиты информации.

Полное наименование - «ГОСТ Р 50922-96. Защита информации. Основные термины и определения».

Гриф

1. Надпись (штамп) на документе или издании, определяющая особый порядок пользования этим документом.
2. Специальная отметка на носителе информации, свидетельствующая о степени конфиденциальности информации, хранимой на этом носителе.

Гамма шифра

Псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму, для зашифрования и расшифрования данных. Данный термин используется только в российской литературе. В иностранной литературе синонимом термина «гамма» является «ключевой поток».

См. также Гаммирование, Шифрование.

Гаммирование

Процесс наложения по определенному алгоритму гаммы шифра на открытый текст. Данный термин используется только в российской литературе. За рубежом синонимом термина «гаммирование» является «поточный шифр».

См. также Гамма шифра, Поточковый шифр.

Гарантии

См. Assurance

Генератор ключевого потока

Алгоритм, вырабатывающий ключевой поток для потоковых криптосистем. Может быть либо детерминированным, что 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 комбинациях регистров сдвига и нелинейных булевых функциях. При построении генераторов ключевого потока часто используют криптографические преобразования блочных шифров, например OFB или счетчиковый метод.

См. также Поточковый шифр, Output Feedback, Счетчиковый метод, Регистр сдвига с обратной связью.

Групповая подпись

Схема цифровой подписи, предложенная в 1991 году 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.

См. также Электронная цифровая подпись.

Генерация ключей

См. Key generation

Д

Достоверность информации

Оценка вероятности отсутствия ошибок в информации.

Доступность системы

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.

См. также Конфиденциальность, Целостность, Доступ.

Доступ

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

См. также Объект, Субъект.

Доступ к ресурсу

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

См. также Доступ.

Дискреционный доступ

См. Избирательный доступ

Диффи-Хеллмана алгоритм

Алгоритм открытого распределения ключей, также называемый экспоненциальным распределением ключей, основанный на использовании односторонней показательной функции $f(x) = a^x \bmod n$. Был опубликован в 1976 г. в статье «Новые направления в криптографии». Применяется для распределения криптографических ключей по незащищенным каналам связи. Для выработки ключа, используемого для шифрования информации пользователи (например, А и В) должны сделать следующее:

1. Пользователи А и В независимо выбирают случайные числа K_A и K_B из интервала от 1 до $p - 1$, причем p – простое число. Числа K_A и K_B называются секретными ключами.
2. Пользователи А и В вычисляют:

$Y_A = g^{K_A} \bmod p$ и $Y_B = g^{K_B} \bmod p$, причем значения g и p являются известными всем абонентам системы обмена сообщениями и $1 < g < p$. Числа Y_A и Y_B называются открытыми ключами. Число g называется генератором.

3. Пользователи А и В обмениваются открытыми ключами по незащищенному каналу связи.
4. По полученным открытым ключам, каждый из пользователей независимо вычисляет секретный параметр К, который и является общим сеансовым секретным ключом, который может использоваться для шифрования.

$$\text{Для пользователя А: } Y_B^{K_A} \bmod p = (g^{K_B})^{K_A} \bmod p = g^{K_B K_A} \bmod p = K$$

$$\text{Для пользователя В: } Y_A^{K_B} \bmod p = (g^{K_A})^{K_B} \bmod p = g^{K_A K_B} \bmod p = K$$

Недостаток схемы Диффи-Хеллмана – необходимость аутентификации открытых ключей пользователей в п.3, т.е. подтверждения того, что ключи Y_A и Y_B действительно выработаны пользователями А и В.

См. также Криптосистема с открытым ключом, Односторонняя функция, Открытое распределение ключей.

Достоверная вычислительная база

Совокупность защитных механизмов вычислительной системы, включая программные и аппаратные компоненты, ответственные за поддержание политики безопасности. ДВБ состоит из одной или нескольких компонентов, которые вместе отвечают за единую политику безопасности в рамках системы. Способность ДВБ корректно проводить единую политику безопасности зависит в первую очередь от механизмов самой ДВБ, а также от корректного управления со стороны администрации системы.

В Руководящих документах Гостехкомиссии РФ данный термин переводится как «комплекс средств защиты».

ДВБ

См. Достоверная вычислительная база

Домен

См. Domain

Достоверный маршрут

См. Trusted path

Джефферсона колесо

Одна из старейших криптографических роторных машин, изобретенная Томасом Джефферсоном и реализующая многоалфавитную подстановку. Представляет собой 36 дисков, свободно вращающихся вокруг общей оси независимо друг от друга. На каждом диске нанесены буквы алфавита. Порядок букв выбирается произвольно и меняется от диска к диску. Основная идея колеса Джефферсона – порождение многоалфавитных подстановок на основе независимо вращающихся дисков.

См. также Роторная машина.

Доска Полибия

См. Полибия квадрат

Декодирование

Процесс преобразования объектного алфавита в исходный.

См. также Кодирование.

Дерево Меркля

См. Merkle's Tree

Дифференциальный криптоанализ

Метод криптоанализа, который может применяться для повторяющихся блочных шифров. Впервые был использован в 1990 году Мэрфи для атаки на алгоритм FEAL-4. В 1991 году был улучшен Бихамом (Biham) и Шамиром (Shamir) для атак на алгоритм DES. 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 счете вычисляется используемый ключ.

См. также Chosen plaintext attack, Линейный криптоанализ, Криптоанализ.

Депонирование ключей

См. Key escrow

Документированная информация

Информация, зафиксированная на материальном носителе и обладающая реквизитами, позволяющими ее идентифицировать.

3

Защита информации

Процесс обеспечения такого свойства информации, как "безопасность".

См. также Система защиты информации, Безопасность информации.

Зашифрование

Процесс применения обратимого преобразования шифра к открытому тексту. Результатом зашифрования является шифртекст.

См. также Расшифрование.

Защищенность

Способность системы противостоять несанкционированному доступу к защищаемой информации, ее искажению или разрушению.

См. также Несанкционированный доступ.

Зона безопасности

Механизм, определенный в браузере Microsoft Internet Explorer компании Microsoft, позволяющий задавать настройки безопасности для групп Internet-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.).

См. также Уровень безопасности.

Злоумышленник

Нарушитель, умышленно действующий из корыстных побуждений.

См. также Нарушитель

И

Идентификация

1. Присвоение идентификаторов субъектам и объектам системы.
 2. Процесс распознавания определенных компонентов системы, обычно с помощью уникальных имен (идентификаторов), воспринимаемых системой.
- См. также Идентификатор.

Идентификатор

Персональное обозначение (имя, код и т.п.), позволяющее однозначно выделить идентифицируемый субъект (объект) среди всех других в полном множестве субъектов (объектов).

См. также Идентификация.

Избирательный доступ

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).

Для описания избирательного доступа применяется матрица доступа. Обычно в системах с избирательным доступом реализуется принцип «все что не разрешено, то запрещено». Решение на доступ субъекта к объекту принимается в соответствии с правами, указанными на в соответствующей ячейке матрицы доступа.

Избирательное управление является основой требований к системам классов С2 и С1 «Оранжевой книги», и к системам классов, начиная с 6-го, Руководящих документов Гостехкомиссии РФ.

См. также Мандатный доступ, Руководящий документ, Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации».

См. также Матрица доступа.

Информация

Сведения о фактах, событиях, процессах 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.

Имитозащита

Механизм защиты информации от навязывания ложных данных. Для обеспечения имитозащиты к зашифрованным данным добавляется имитовставка.

См. также Имитовставка, Message Authentication Code.

Имитовставка

Последовательность данных фиксированной длины, полученная по определенному правилу из открытого текста и ключа. В зарубежной литературе данному термину соответствует термин «код целостности сообщений» («message integrity check»).

См. также Имитозащита, Message Authentication Code.

Инструктивные указания Государственного Арбитража СССР № И-1-4

Инструктивные указания Государственного Арбитража СССР № И-1-4, утвержденные 29 июня 1979 года. Разрешают использовать в качестве доказательств по арбитражным судам документы, подготовленные с помощью электронно-вычислительной техники.

К

Ключ криптографический

Совокупность данных, определяющих конкретное преобразование из множества преобразований шифра.

См. также Криптографическое преобразование, Шифр.

Код

1. Множество преобразований элементов открытого текста (буквы, сочетания букв, слова и т.п.) группами символом (букв, цифр или других знаков). Является специальным типом шифра.

См. также Шифр.

2. Правило преобразования сообщения из одного (исходного) алфавита в другой, (объектный) обычно без каких-либо потерь информации.

См. также Кодирование.

Кодирование

Процесс преобразования исходного алфавита в объектный.

См. также Код, Шифрование.

Криптография

Наука о методах обеспечения секретности и/или подлинности данных при их передаче по каналам связи или хранении.

См. также Криптоанализ, Криптология, Стеганография.

Криптографическая система

Семейство выбираемых с помощью ключа обратимых преобразований, которые преобразуют открытый текст в шифртекст и обратно.

См. также Криптографическое преобразование.

Контроль доступа

Процесс, который ограничивает доступ к ресурсам автоматизированной системы в соответствии с требуемой моделью защиты.

См. также Доступ к ресурсу.

Конфиденциальность

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.

См. также Доступность, Целостность.

Конфиденциальная информация

1. Информация, имеющая ограничения на право доступа к ней со стороны пользователей и, как следствие, требующая защиты от несанкционированного к ней доступа.
2. Служебная, профессиональная, промышленная, коммерческая или иная информация, правовой режим которой устанавливается ее собственником на основе законов о коммерческой, профессиональной (промышленной) тайне, государственной службе и других законодательных актов. Требует защиты.

См. также Информация.

Концепция защиты информации

Документ, определяющий общую систему взглядов на проблему защиты информации 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. Положения концепции распространяются на филиалы, подразделения (отделы, департаменты) организации и другие учреждения (организации, предприятия), связанные с обработкой в автоматизированной системе информации, составляющей государственную, служебную, банковскую, коммерческую тайну, а также которые заинтересованы в обеспечении целостности, доступности и конфиденциальности информации.

Криптоанализ

Наука о методах раскрытия и/или подделки данных. В России под термином «криптоанализ» ранее понималось расшифрование шифртекста.

См. также Криптология, Криптография, Расшифрование, Adaptive chosen ciphertext attack, Brute-force search, Birthday attack, Chosen plaintext attack, Chosen ciphertext attack, Chosen message attack, Ciphertext only attack, Chosen key attack, Guessed plaintext attack, Known plaintext attack, Middleperson attack, Purchase key attack, Rubber hose cryptanalysis, Дифференциальный криптоанализ, Линейный криптоанализ.

Криптология

Наука о создании и анализе систем безопасном хранении и передаче информации по каналам связи. Криптологию принято делить на две части – криптографию и криптоанализ.

См. также Криптография, Криптоанализ.

Класс защищенности

Определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации

См. также Несанкционированный доступ, Руководящий документ.

Ключевая система

Совокупность правил, определяющих порядок генерации, распределения, использования, хранения, смены, уничтожения и восстановления криптографических ключей.

См. также Ключ криптографический.

Канальное шифрование

Защита информации, передаваемой средствами телекоммуникаций криптографическими методами; шифрование осуществляется в канале связи между двумя узлами (которые могут быть промежуточными на пути от отправителя к получателю).

См. также Абонентское шифрование, Шифрование.

Красная книга

1. См. The Trusted Network Interpretation of Department of Defense Trusted Computer System Evaluation Guidelines
2. См. X.400

Компрометация информации

Утечка или разглашение конфиденциальной информации, либо получение ее неавторизованными субъектами.

Криптосистема с секретным ключом

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. Недостатком симметричных систем является тот факт, что получатель не может расшифровать информацию пока не получит по надежному каналу секретный ключ. Для решения проблемы распределения ключей по незащищенным каналам была разработана модель открытого распределения ключей.

Криптографические системы с секретным ключом делятся на блочные и поточные криптосистемы.

См. также Блочный шифр, Поточный шифр, Открытое распределение ключей, Криптосистема с открытым ключом.

Криптосистема с открытым ключом

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. Пользуясь открытым ключом любой из абонентов может послать защищенное сообщение автору открытого ключа. При этом расшифровать это сообщение можно только имея секретный ключ, соответствующий открытому. Такие криптосистемы, также называются

двуключевыми и асимметричными. Криптосистемы с открытым ключом обеспечивают только практическую стойкость, в отличие от симметричных криптосистем, которые могут обеспечивать не только практическую, но и теоретическую стойкость. Криптосистемы с открытым ключом основываются на т.н. односторонних (однонаправленных, необратимых) функциях.

На сегодняшний день высокоскоростных алгоритмов с открытым ключом (по сравнению с симметричными системами) не найдено. Поэтому одним из основных применений таких систем является управление ключами и создание электронной цифровой подписи.

См. также Односторонняя функция, Электронная цифровая подпись, Открытое распределение ключей, RSA, Цифровой конверт.

Квадрат Вижинера

См. Вижинера квадрат

Казиски метод

Метод криптоанализа, позволяющий вычислять период многоалфавитных криптосистем при помощи обнаружения одинаковых слов в шифртексте. Если период многоалфавитной криптосистемы становится известным, то криптоанализ может быть сведен к криптоанализу одноалфавитных систем.

См. также Криптоанализ.

Квадрат Полибия

См. Полибия квадрат

Кардано решетка

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°, открывая тем самым новые, незаполненные ячейки.

См. также Криптографическая система.

Коды, исправляющие ошибки

Избыточные коды, использование которых позволяет с большой вероятностью не только обнаруживать, но и исправлять возникшие при передаче информации ошибки

См. также Коды Гоппы.

Коды Гоппы

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.

См. также Коды, исправляющие ошибки.

Криптографический протокол

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.

См. также Протокол с арбитром, Протокол с третейским судьей, Протокол, самообеспечивающий законность, Протокол отрицания.

Криптографическое преобразование информации

Процесс преобразования информации, основанный на применении криптографических методов (зашифрование и расшифрование, выработка и проверка электронной цифровой подписи, выработка и проверка хэш-функции).

См. также Зашифрование, Расшифрование, Электронная цифровая подпись, Хэш-функция.

Квантовая криптография

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.

Данный механизм был опубликован в конце 70-х гг. В настоящий момент практического применения квантовая криптография не имеет; используется только в качестве эксперимента.

Криптосистема с временным раскрытием

Криптографическая система, которая позволяет расшифровать защищенное сообщение только по истечении заданного интервала времени. В настоящий момент существует два варианта реализации таких систем:

- 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.

См. также Криптографическая система, Шарады с временным замком.

Криптосистема с эллиптическими кривыми

Криптосистема, основанная на математическом аппарате эллиптических кривых из теории чисел.

См. также Криптографическая система.

Криптосистема МакЭлиса

Криптосистема, основанная на кодах, исправляющих ошибки. Предложена в 1978 году Робертом МакЭлисом. Ей присущи два недостатка: большая длина ключа и большая избыточность (длина шифртекста вдвое превышает длину сообщения). В 1991 году два российских криптографа «взломали» систему МакЭлиса [6].

См. Коды, исправляющие ошибки, Коды Гоппы, Криптографическая система.

Криптосистема Нидеррайтера

Криптосистема, основанная на кодах, исправляющих ошибки. Предложена в 1986 г. Г. Нидеррайтером.

См. Коды, исправляющие ошибки, Коды Гоппы, Криптографическая система.

Криптосистема Габидулина

Криптосистема, основанная на кодах, исправляющих ошибки в ранговой метрике. Предложена в 1992 г. Э.М. Габидулиным.

См. Коды, исправляющие ошибки, Коды Гоппы, Криптографическая система.

Криптосистема Крука

Криптосистема, основанная на кодах, исправляющих ошибки. Предложена Е. Круком, для устранения недостатков криптосистемы МакЭлиса.

См. Коды, исправляющие ошибки, Коды Гоппы, Криптосистема МакЭлиса, Криптографическая система.

Криптосистема Вернама

См. Одноразовый блокнот

Коллизия

Событие, при котором хэш-функции от разных сообщений совпадают.

См. также Хэш-функция

Код аутентификации сообщения

См. Message Authentication Code

Код целостности сообщений

См. Имитовставка

Контроль эффективности защиты информации

Проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты.

См. также Показатель эффективности защиты информации.

Л

Лицензирование

Деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации

См. также Лицензия, Лицензиат, Лицензиар, Государственная техническая комиссия при Президенте РФ.

Лицензия

Оформленное соответствующим образом разрешение на право проведения тех или иных работ в области защиты информации.

См. также Лицензиат, Лицензирование, Лицензиар, Государственная техническая комиссия при Президенте РФ.

Лицензиат

Сторона, получившая право (лицензию) на проведение работ в области защиты информации.

См. также Лицензия, Лицензирование, Лицензиар, Государственная техническая комиссия при Президенте РФ.

Лицензиар

Сторона, выдавшая лицензию на право проведения работ в области защиты информации.

См. также Лицензия, Лицензирование, Лицензиат, Государственная техническая комиссия при Президенте РФ.

Люк

Скрытая или недокументированная точка входа в автоматизированную систему. Может применяться для обхода системы защиты.

Логическая бомба

См. Бомба логическая

Линейный криптоанализ

Метод криптоанализа, который может применяться для блочных шифров. Впервые был предложен в 1992 году Матсуи (Matsui) и Ямагиши (Yamagishi) для атак на алгоритм FEAL. В 1993 году был расширен Матсуи для атак на алгоритм DES. Данный метод криптоанализа базируется на методе криптоанализа по известному открытому тексту. В 1994 году Лангфорд (Langford) и Хеллман предложили атаку, называемую дифференциально-линейным криптоанализом.

См. также Дифференциальный криптоанализ, Known plaintext attack, Криптоанализ.

М

Мандатный доступ

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.

Мандатное управление доступом подразумевает, что:

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

Каждый объект кроме базового уровня безопасности имеет еще и текущий уровень, который может изменяться в зависимости от меток критичности тех объектов, к которым субъект имеет доступ в данный момент.

Для моделирования мандатного доступа используется Белла-Лападулла модель.

Основное назначение мандатного управления доступом – обеспечение безопасного доступа субъектов системы к объектам с разными уровнями критичности и предотвращению утечки информации с верхних уровней должностной иерархии на нижний, а также блокирование возможных проникновений с нижнего уровня на верхний.

Избирательное управление является основой требований к системам классов В1 «Оранжевой книги», и к системам классов, начиная с 4-го, Руководящих документов Гостехкомиссии РФ.

См. также Избирательный доступ, Руководящий документ, Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации».

Маскарад

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.

Морально-этические меры защиты информации

Традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Матрица доступа

Предназначена 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.

См. также Избирательный доступ.

Мандат

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.

См. также Доступ.

Минимум привилегий

Один из основополагающих принципов организации системы защиты, гласящий, что каждый субъект должен иметь минимально возможный набор привилегий, необходимый для решения поставленных перед ним задач. Следование этому принципу предохраняет от нарушений, возможных в результате злого умысла, ошибки или несанкционированного использования привилегий.

См. также Доступ, Несанкционированный доступ, Привилегии.

Многоуровневая безопасность

См. Multilevel security

Монитор ссылок

См. Reference monitor concept

Метка конфиденциальности

Элемент, который характеризует конфиденциальность информации, содержащейся в объекте.

См. также Конфиденциальность, Мандатный доступ.

Многоуровневая защита

Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам с различными уровнями безопасности.

См. также Право доступа, Уровень безопасности.

Модель нарушителя

Абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа, отражающее его практические и теоретические возможности, априорные знания, время и место действия и т.п.

См. также Нарушитель, Злоумышленник, Правило доступа.

Модель защиты

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

См. также Несанкционированный доступ.

Многоуровневая криптография

Механизм, предложенный Р. Райвестом, 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. Необходимость в создании таких криптосистем появилась в связи с введением в США экспортных ограничений на «сильную» криптографию. Многоуровневые криптосистемы позволяют, с одной стороны, обеспечить необходимый уровень защищенности для коммерческих организаций, а с другой стороны – дают возможность государственным органам (в частности, NSA) при необходимости могут провести атаку «brute force» на шифртексты. Это достигается за счет того, что объем перебора, выполняемый для первого ключа (первый уровень сложности), превышает объем перебора для раскрытия любого следующего ключа. При этом любой ключ из заданного ключевого пространства должен удовлетворять первому уровню сложности.

См. также Криптосистема с секретным ключом, Brute-force attack, Capstone.

Н

Несанкционированный доступ

Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа.

См. также Правила разграничения доступа.

НСД

См. Несанкционированный доступ

Несанкционированное действие

Действие субъекта в нарушение установленных в системе правил обработки информации.

См. также Несанкционированный доступ.

Нарушитель

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 (чисто агентурные методы получения сведений, технические средства перехвата без модификации компонентов системы, штатные средства и недостатки систем защиты, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ и т.п.).

См. также Модель нарушителя, Несанкционированный доступ, Злоумышленник.

Национальный Центр Компьютерной Безопасности

См. National Computer Security Center

Носители информации

Материальные объекты (в т.ч. и люди), предназначенные для хранения, обработки и передачи информации.

Нормы эффективности защиты информации

Значения показателей эффективности защиты информации, установленные нормативными документами.

См. также Показатель эффективности защиты информации.

О

Открытый ключ

Ключ, используемый в асимметричной криптосистеме и доступный всем пользователям системы.

См. также Криптосистема с открытым ключом, Секретный ключ.

Открытый текст

Исходное защищаемое сообщение.

См. также Шифртекст.

Обнаружение атак

Механизм, используемый для обнаружения атак на объекты системы.

См. также Анализ защищенности

Обработка информации в АС

Совокупность операций (сбор, накопление, хранение, преобразование, отображение, выдача и т.п.), осуществляемых над информацией (сведениями, данными) с использованием средств АС.

Объект

Пассивный компонент системы, хранящий, принимающий или передающий информацию, доступ к которому регламентируется правилами разграничения доступа.

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.).

См. также Субъект.

Организационные меры защиты информации

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.

См. также Технические меры защиты информации, Правовые меры защиты информации, Физические меры защиты информации.

Отказ в обслуживании

Любое действие или последовательность действий, которая приводит любую часть системы к выходу из строя, при котором та перестают выполнять свои функции. Причиной может быть несанкционированный доступ, задержка в обслуживании и т.д.

Оранжевая книга

См. Orange book

Оконечное шифрование

См. Абонентское шифрование

Односторонняя функция

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, т.к. расшифровать текст, зашифрованный с их помощью, не сможет даже законный владелец. В криптографии используются однонаправленные функции с секретом.

См. также Криптосистема с открытым ключом, Диффи-Хеллмана алгоритм, Односторонняя функция с секретом,

Односторонняя функция с секретом

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.

Исследования таких функций проводится, в основном, по следующим направлениям:

- дискретное возведение в степень – алгоритм Диффи-Хеллмана и др.;
- факторизация простых чисел – алгоритм RSA и др.;
- коды, исправляющие ошибки – алгоритм МакЭллиса и др.;
- задачи NP-полноты – задача об «укладке ранца» и др.

См. также Криптосистема с открытым ключом, Открытое распределение ключей, Диффи-Хеллмана алгоритм, Криптосистема МакЭллиса, RSA

Открытое распределение ключей

Механизм распределения криптографических ключей по незащищенным каналам связи. Данный механизм был впервые предложен в 1976 году американскими учеными Диффи и Хеллманом и базировался на задаче дискретного логарифмирования. Несмотря на то, что идеи открытого распределения ключей и шифрования с открытым ключом были

предложены одновременно, авторы не смогли предложить конкретную реализацию системы шифрования с открытым ключом. Системы, реализующие принцип открытых ключей для шифрования появились позже.

См. также Криптосистема с открытым ключом, Односторонняя функция, Диффи-Хеллмана алгоритм.

Одноразовая цифровая подпись

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), т.к. каждая подпись используется только один раз.

См. также Merkle's Tree, Электронная цифровая подпись.

Одноразовый блокнот

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

Данная криптосистема непрактична, т.к. приходится вырабатывать ключи большого размера. В основном, она используется в военных и дипломатических целях. Основной недостаток – трудности в управлении ключами.

См. также Криптографическая система, Поточковый шифр.

П

Пароль

Идентификатор субъекта системы, который является его (субъекта) секретом.

Полномочия

Право субъекта (объекта) системы осуществлять доступ к защищаемым данным.

Правило доступа

Совокупность правил, регламентирующих порядок и условия доступа к защищаемой информации и ее носителям.

См. также Право доступа.

Право доступа

Совокупность правил доступа к защищаемой информации, установленных правовыми документами или собственником, владельцем информации.

См. также Правило доступа.

Профиль полномочий

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.

См. также Полномочия, Матрица доступа.

Привилегии

См. Полномочия

План защиты

Документ, определяющий реализацию системы защиты организации и необходимый в повседневной работе.

См. также Концепция защиты информации.

Политика безопасности

Набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение защищаемой информации в системе. Она охватывает все особенности процесса обработки информации, определяя поведение системы в различных ситуациях.

См. также Концепция защиты информации, План защиты.

Подпись кода

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.

Существует две основных реализации данного механизма – Object Signing компании Netscape и Authenticode компании Microsoft.

См. также Authenticode, Object Signing, Аутентификация.

Потоковый шифр

Криптографическое преобразование, при котором открытый текст разбивается на символы или биты и каждый знак p_i зашифровывается с помощью обратимого преобразования, выбранного в соответствии со знаком k_i ключевого потока. В отличие от блочных шифров, в потоковых криптосистемах не происходит распространения ошибок или оно ограничено.

В отечественной практике потоковые криптосистемы называются системами гаммирования. К поточным криптосистемам можно отнести ГОСТ 28147-89 (режим гаммирования и гаммирования с обратной связью), DES (режимы CFB и OFB) и некоторые другие. Поточные криптосистемы делятся на синхронизирующиеся и самосинхронизирующиеся поточные криптосистемы. Очень часто потоковые криптосистемы основаны на алгоритмах блочного шифрования, преобразованных для специального применения.

См. также Блочный шифр, ГОСТ 28147-89, Cipher Feedback, Output Feedback, Гаммирование.

Правила разграничения доступа

Совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе.

См. также Право доступа.

Правовые меры защиты информации

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.

См. также Организационные меры защиты информации, Технические меры защиты информации, Физические меры защиты информации.

Полномочный доступ

См. Мандатный доступ

Подотчетность

См. Accountability

План обеспечения непрерывной работы и восстановления

План реагирования на опасные ситуации, резервного копирования и последующих восстановительных процедур, являющийся частью программы защиты и обеспечивающий доступность основных ресурсов системы и непрерывность обработки в кризисных ситуациях.

См. также План защиты.

Повторное использование объекта

См. Object reuse

Правило Киркоффа

Стойкость шифра должна определяться только секретностью ключа.

См. также Стойкость, Ключ криптографический, Шифр.

Полибия квадрат

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.

См. также Криптографическая система.

Показатель защищенности

Характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники

См. также Класс защищенности, Руководящий документ.

Протокол с арбитром

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.

Арбитр является самым узким местом данных протоколов. Арбитры требуют дополнительных материальных затрат на поддержание своего функционирования, а также некоторых временных издержек, т.к. арбитр должен контролировать любое действие участников протокола. Увеличение числа арбитров ведет к увеличению временных и материальных затрат.

См. также Криптографический протокол.

Протокол с третьей стороной

Данные протоколы аналогичны протоколам с арбитром, но в отличие от последних, третьей стороной является только в случае возникновения спорных ситуаций между участниками протокола. Третьей стороной, в отличие от арбитра, не участвует напрямую в

протоколе, однако существуют данные, которые позволяют третейскому судье определить обман.

См. также Криптографический протокол.

Протокол, самообеспечивающий законность

Один из лучших типов криптографических протоколов, позволяющих обойтись без третьей стороны. В данном типе протокола он сам гарантирует соблюдение всех правил. Такой протокол построен так, что в случае возникновения обмана с одной стороны, другая сторона всегда может определить это.

См. также Криптографический протокол.

Протокол отрицания

Тип протокола, не позволяющий подписывающему лицу отказаться от подписанного сообщения.

См. также Криптографический протокол, Бесспорная подпись.

Полный перебор

См. Brute-force search

Посредник

См. Проху

Показатель эффективности защиты информации

Мера или характеристика для оценки эффективности защиты информации.

См. также Эффективность защиты информации.

Пользователь информации

1. Субъект, обращающийся к информационной системе или посреднику 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 установленными правами и правилами доступа к информации либо с их нарушением.

См. также Владелец информации, Собственник информации.

Потребитель информации

См. Пользователь информации

Постановление Правительства РФ №1233

Постановление Правительства РФ, утвержденное 3 ноября 1994 года. Устанавливает порядок обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти.

Постановление Правительства РФ №333

Постановление Правительства РФ, утвержденное 15 апреля 1995 года. Устанавливает порядок лицензирования деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны.

Постановление Правительства РСФСР №35

Постановление Правительства РСФСР, утвержденное 5 декабря 1991 года. Определяет перечень сведений, которые не могут составлять коммерческую тайну.

Постановление Правительства РФ №608

Постановление Правительства РФ, утвержденное 26 июня 1996 года. Устанавливает порядок сертификации средств защиты информации.

Письмо Высшего Арбитражного Суда РФ № С1-7/ОП-587

Письмо Высшего Арбитражного Суда РФ № С1-7/ОП-587 от 19 августа 1994 года, определяющее порядок подтверждения обстоятельств арбитражного дела доказательствами, изготовленными и подписанными с помощью средств электронно-вычислительной техники, в которых использована система цифровой (электронной) подписи.

Письмо Высшего Арбитражного Суда РФ № С1-7/ОЗ-316

Письмо Высшего Арбитражного Суда РФ № С1-7/ОЗ-316 от 7 июня 1995 года, разъясняющее порядок применения Федерального закона "Об информации, информатизации и защите информации" и определяющее порядок подтверждения обстоятельств арбитражного дела доказательствами, изготовленными и подписанными с помощью средств электронно-вычислительной техники, в которых использована система цифровой (электронной) подписи.

Р

Разграничение доступа

Порядок использования ресурсов системы, при котором субъекты получают доступ к объектам в строгом соответствии с установленными правилами.

См. также Правила разграничения доступа.

Расшифрование

Процесс обратного преобразования шифртекста в открытый текст.

См. также Зашифрование, Криптографическое преобразование.

Распознавание атаки

См. Обнаружение атак

Регламентация

Создание таких условий обработки информации при которых возможности несанкционированного доступа к ней сводилась бы к минимуму.

См. также Несанкционированный доступ.

Руководящий документ

Документ, излагающий систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от несанкционированного доступа (НСД), являющейся частью общей проблемы безопасности информации.

См. также Государственная техническая комиссия при Президенте РФ, Руководящий документ «Концепция защиты СВТ и АС от НСД к информации», Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения», Руководящий документ «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники», Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации», Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», Руководящий документ «Защита информации. Специальные защитные знаки. Классификация и общие требования»

Радужная серия

См. Rainbow series

Роторная машина

Криптографическая машина, состоящая из дисков, свободно вращающихся вокруг общей оси. Бывают механическими или электромеханическими. Диски (роторы) машины перемещаются одно относительно другого, создавая тем самым на каждом такте уникальное сочетание угловых положений. Если все диски были бы неподвижными, то роторная машина представляла бы собой простую замену, эквивалентную замене, реализуемую одним диском. При большом количестве дисков (обычно 5 – 10) и правильно выбранном законе псевдослучайного движения дисков роторная машина обеспечивает достаточно высокую криптостойкость.

Самой известной из роторных машин является машина С-36, также известная как М-209 Converter.

См. также С-36.

Решетка Кардано

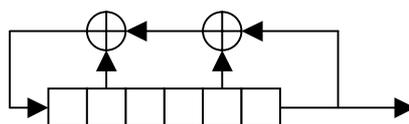
См. Кардано решетка

Разделение секретов

См. Secret Sharing Scheme

Регистр сдвига с обратной связью

Механизм для генерации последовательности бит. Состоит из ряда ячеек, которые заполняются вектором инициализации, который наиболее часто является секретным ключом. Содержимое ячеек регистра регулируется по времени и в каждый момент синхронизации содержание ячеек регистра перемещается вправо на одну позицию и складывается по модулю 2 (операции XOR) с содержимым ячейки в крайней левой позиции.



Используется как один из элементов в многочисленных поточных криптосистемах.
См. также Криптографическая система, Поточковый шифр.

Распределение ключей

См. Key distribution

Решение Гостехкомиссии и ФАПСИ №10

Решение Государственной технической комиссии при Президенте РФ и Федерального Агентства Правительственной Связи при Президенте РФ, утвержденное 27 апреля 1994 года. Устанавливает основные принципы, организационную структуру системы государственного лицензирования деятельности юридических лиц - предприятий, организаций и учреждений независимо от их организационно-правовой формы по защите информации, циркулирующей в технических средствах и помещениях, а также порядок лицензирования и контроля за деятельностью предприятий, получивших лицензию.

См. также Государственная техническая комиссия при Президенте РФ, Лицензирование, Федеральное агентство правительственной связи и информации.

Руководящий документ «Концепция защиты СВТ и АС от НСД к информации»

Документ, разработанный и утвержденный Гостехкомиссией РФ 30 марта 1992 года. Предназначен для заказчиков, разработчиков и пользователей средств вычислительной техники (СВТ) и автоматизированных систем, которые используются для обработки, хранения и передачи требующей защиты информации.

Концепция является методологической базой нормативно-технических и методических документов, направленных на решение следующих задач:

- выработка требований по защите СВТ и АС от НСД к информации;
- создание защищенных СВТ и АС, т.е. защищенных от НСД к информации;
- сертификация защищенных СВТ и АС.

См. также Государственная техническая комиссия при Президенте РФ.

Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения»

Документ, разработанный и утвержденный Гостехкомиссией РФ 30 марта 1992 года. Устанавливает термины и определения понятий в области защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.

См. также ГОСТ Р 50922-96, Государственная техническая комиссия при Президенте РФ.

Руководящий документ «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники»

Документ, разработанный и утвержденный Гостехкомиссией РФ 30 марта 1992 года. Положение устанавливает единый на территории Российской Федерации порядок исследований и разработок в области:

- защиты информации, обрабатываемой автоматизированными системами различного уровня и назначения, от несанкционированного доступа;
- создания средств вычислительной техники общего и специального назначения, защищенных от утечки, искажения или уничтожения информации за счет НСД, в том числе программных и технических средств защиты информации от НСД;
- создания программных и технических средств защиты информации от НСД в составе систем защиты секретной информации в создаваемых АС.

См. также Государственная техническая комиссия при Президенте РФ.

Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации.»

Классификация автоматизированных систем и требования по защите информации»

Документ, разработанный и утвержденный Гостехкомиссией РФ 30 марта 1992 года. Устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов.

См. также Государственная техническая комиссия при Президенте РФ, Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации».

Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации»

Документ, разработанный и утвержденный Гостехкомиссией РФ 30 марта 1992 года. Устанавливает классификацию средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

См. также Государственная техническая комиссия при Президенте РФ, Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»

Документ, разработанный и утвержденный Гостехкомиссией РФ 25 июля 1997 года. Устанавливает классификацию межсетевых экранов по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

См. также Государственная техническая комиссия при Президенте РФ, Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации».

Руководящий документ «Защита информации. Специальные защитные знаки. Классификация и общие требования»

Документ, разработанный и утвержденный Гостехкомиссией РФ 25 июля 1997 года. устанавливает классификацию по классам защиты специальных защитных знаков, предназначенных для контроля доступа к объектам защиты, а также для защиты документов от подделки.

См. также Государственная техническая комиссия при Президенте РФ.

С

Сертификация СЗИ

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.

См. также Лицензирование, Государственная техническая комиссия при Президенте РФ.

Сертификат соответствия

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.

См. также Лицензия, Государственная техническая комиссия при Президенте РФ, Сертификация СЗИ.

Система защиты информации

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 АС (циркулирующей в АС информации).

См. также Технические меры защиты информации, Правовые меры защиты информации, Организационные меры защиты информации.

Система криптографической защиты информации

Система, осуществляющая криптографическое преобразование информации для обеспечения ее безопасности.

См. также Криптографическое преобразование.

Система обнаружения атак

Техническое или программное средство, предназначенное или используемое для обнаружения атак на ресурсы системы.

См. также Обнаружение атак.

Система анализа защищенности

Техническое или программное средство, предназначенное или используемое для анализа защищенности технических средств или АС.

См. также Анализ защищенности.

Скремблер

Аналоговый речевой шифратор.
См. также Шифрование.

Средство защиты информации

Технические, криптографические, программные и другие средства, предназначенный для защиты информации, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

См. также Технические меры защиты информации, Эффективность защиты информации.

Стойкость

Способность противостоять попыткам криптоаналитика дешифровать шифртекст, раскрыть ключи шифра или нарушить целостность и/или подлинность информации. Различается практическая и теоретическая стойкость. Криптосистема теоретически стойкая, если криптоаналитик не может уточнить распределение вероятностей возможных открытых текстов по имеющемуся у него шифртексту. Криптосистема практически стойкая, если она не может быть вскрыта в течение реального времени всеми общедоступными методами.

См. также Криптоанализ, Криптографическая система.

Сниффинг

См. Sniffing

Спуффинг

См. Spoofing

Субъекты информационных отношений

Государство, государственные органы, государственные, общественные или коммерческие организации (объединения) и предприятия (юридические лица), отдельные граждане (физические лица) и иные субъекты, взаимодействующие с целью совместной обработки информации.

По отношению к информации, обрабатываемой в АС, 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 АС и участников процессов обработки и передачи информации и т.д.

Субъект

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.

См. также Объект, Domain.

«Салями» атака

См. Salami attack

Скрытые каналы

См. Covert channels

Скрытый временной канал

См. Covert timing channel

Скрытый канал с памятью

См. Covert storage channel

Сборка мусора

Атака, заключающаяся в поиске информации, остающейся в оперативной памяти или на накопителях информации после работы субъекта или объекта системы.

См. также Атака.

Список контроля доступа

Представление матрицы доступа по столбцам – каждому объекту соответствует список субъектов вместе с их правами.

См. также Матрица доступа.

Сторнетта-Хабера алгоритм

Алгоритм, разработанный учеными Bell Communications Research, обеспечивает подпись документов по времени без возможности их подделки.

См. также Timestamping.

Стеганография

Наука о методах скрытия самого факта передачи сообщения. Примером стеганографии является акростих.

См. также Криптография.

Синхронизирующаяся потоковая криптосистема

В синхронизирующихся криптосистемах ключевой поток вырабатывается независимо от открытого текста и шифртекста. Поэтому, если какой-либо символ шифртекста потерян при передаче, то получатель должен пересинхронизировать свой ключевой поток, отбросив соответствующий символ ключевого потока для правильного расшифрования последующих знаков шифртекста. Для выработки ключевого потока применяются генераторы ключевого потока. У военных такие системы называются ключ с автоключом (key auto key).

Примером синхронизирующейся потоковой криптосистемы является ГОСТ 28147-89 в режиме гаммирования.

См. также Генератор ключевого потока, ГОСТ 28147-89, Output Feedback, Поточковый шифр.

Самосинхронизирующаяся потоковая криптосистема

Данные потоковые криптосистемы характеризуются тем, что каждый знак ключевого потока в любой момент времени определяется фиксированным числом предшествующих знаков шифртекста. Преимущество данных систем в том, что как только на приемном конце принят неискаженный отрезок шифртекста длины n , то значение соответствующего знака ключевого потока также будет определено. У военных такие системы называются шифры с автоключом (cipher text auto key).

Примером самосинхронизирующейся потоковой криптосистемы является ГОСТ 28147-89 в режиме гаммирования с обратной связью.

См. также ГОСТ 28147-89, Cipher Feedback, Поточковый шифр, Синхронизирующаяся потоковая криптосистема.

Счетчиковый метод

Этот режим использования блочного шифра похож на режим OFB, но на вход регистра подается не результат шифрования, а некий счетчик, состояние которого увеличивается на константу, обычно единицу. Этот режим использования блочного шифра является примером синхронизирующейся потоковой криптосистемы.

Примером счетчикового метода является режим гаммирования в ГОСТ 28147-89.

См. также ГОСТ 28147-89, Блочный шифр, Output Feedback, Поточковый шифр, Синхронизирующаяся потоковая криптосистема.

Совершенная секретность

Условие, заключающееся в том, что открытый текст и шифртекст статистически независимы и получение (перехват) шифртекста не дает криптоаналитику дополнительной информации об открытом тексте. Для совершенно секретных криптосистем должно выполняться условие (граница Шеннона): неопределенность секретного ключа должна быть не меньше неопределенности шифруемого с его помощью текста. Другими словами, ключ не должен быть короче открытого текста.

Системы с длиной ключа равной длине шифруемого текста не нашли широкого распространения в коммерческом секторе из-за неудобства, связанного с хранением ключей большого объема.

См. также Ключ криптографический, Криптоанализ.

Слепая подпись

См. Blind signature scheme

Самопроверяющаяся подпись

См. Self-authenticating signature scheme

Сертификат ключа

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. Наиболее известный и распространенный формат сертификата описан в стандарте ITU-T X.509.

См. также X.509, Открытый ключ.

Список аннулированных сертификатов

Список сертификатов, которые были отменены прежде, чем истекло время их действия.

См. также Сертификат, Timestamping.

Сервер-посредник

См. Proxy Server

Секретный ключ

1. Ключ, используемый в асимметричной криптосистеме и известный, как правило, только одному объекту системы.

См. также Криптосистема с открытым ключом.

2. Ключ, используемый в симметричной криптосистеме и разделяемый между объектами или субъектами, которые устанавливают защищенное взаимодействие.

См. также Криптосистема с секретным ключом.

Собственник информации

1. Субъект, реализующий в полном объеме полномочия владения, пользования, распоряжения информацией в соответствии с 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.

См. также Владелец информации, Пользователь информации.

Т

Троянский конь

Программа, выполняющая в дополнение к основным функциям, неописанные в документации действия. Данные действия могут использовать законные полномочия субъекта системы для осуществления несанкционированного доступа.

См. также Маскарад, Бомба логическая.

Технические меры защиты информации

Различные электронные устройства и специальные программы, входящие в состав АС, 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.).

См. также Организационные меры защиты информации, Правовые меры защиты информации, Физические меры защиты информации.

Туннелирование

См. Virtual Private Network.

У

Уязвимость АС

Любая характеристика информационной системы, использование которой нарушителем может привести к реализации угрозы.

См. также Атака, Нарушитель, Угроза АС.

Уязвимость субъекта информационных отношений

Потенциальная подверженность субъекта нанесению ущерба его жизненно важным интересам посредством воздействия на критичную для него информацию, ее носители и процессы ее обработки.

См. также Уязвимость АС.

Уязвимость информации

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

См. также Уязвимость АС.

Угроза АС

Потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба (материального, морального или иного) ресурсам АС.

См. также Уязвимость АС, Атака.

Угроза интересам субъектов информационных отношений

Потенциально возможное событие, действие, процесс или явление, которое посредством воздействия на информацию и другие компоненты АС может привести к нанесению ущерба интересам данных субъектов.

См. также Угроза АС.

Угроза безопасности информации

Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию.

См. также Угроза АС, Доступность, Конфиденциальность, Целостность.

Управление ключами

См. Ключевая система

Управление доступом

См. Контроль доступа

Уровень безопасности

См. Мандатный доступ

Уровень прозрачности

Максимальный уровень безопасности, доступ к которому разрешен данному субъекту правилами модели Белла-Лападулла.

См. также Белла-Лападулла модель.

Уровень доступа

Иерархическая часть метки уровня безопасности, используемая для идентификации критичности данных или прозрачности субъектов. Уровень доступа вместе с неиерархическими категориями составляет уровень безопасности.

См. также Уровень безопасности, Уровень прозрачности.

Уровень полномочий

Совокупность прав доступа субъекта системы.

См. также Уровень безопасности

Уровень привилегий

См. Уровень безопасности

Установление подлинности

См. Аутентификация

Указ Президента РФ №334

Указ Президента РФ, утвержденный 3 апреля 1995 года. Определяет меры по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации.

В действительности монополизирует деятельность по обеспечению криптографической защиты информации в рамках ФАПСИ.

См. также Федеральное агентство правительственной связи и информации, Шифровальные средства.

Указ Президента РФ №188

Указ Президента РФ, утвержденный 6 марта 1997 года. Определяет перечень сведений конфиденциального характера.

Ф

Федеральное агентство правительственной связи и информации

Создано Указом Президента РФ от 24 декабря 1991 года №313 на базе бывших Комитета правительственной связи при Президенте РСФСР (КПС), Государственного информационно-вычислительного центра при Государственной технической комиссии по чрезвычайным ситуациям (Госцентр СССР) и Московского НИИ электротехники Научно-производственного объединения «Автоматика». В свою очередь основу КПС составили бывшие 8 Главное управление, 16 Управление и Управление правительственной связи КГБ СССР [21].

ФАПСИ ведает вопросами организации и обеспечения правительственной связи, иных видов специальной связи, является головной организацией в стране в части организации и обеспечения комплексной криптографической защиты информационно-телекоммуникационных систем и баз данных органов власти Российской Федерации.

См. также Криптография, Государственная техническая комиссия при Президенте РФ.

ФАПСИ

См. Федеральное агентство правительственной связи и информации

Физические меры защиты информации

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 АС и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации.

См. также Организационные меры защиты информации, Правовые меры защиты информации, Технические меры защиты информации.

Х

Хэш-функция

Функция, преобразующая текст произвольной длины в текст фиксированной (в большинстве случаев меньшей) длины. Базовые требования к криптографической хэш-функции:

- на вход функции может подаваться текст любой длины;
- на выходе функции получается текст фиксированной длины;
- хэш-функция достаточно просто вычисляется для любого сообщения;
- хэш-функция односторонняя;
- функция свободна от коллизий.

Основное применение хэш-функции нашли в схеме цифровой подписи. Т.к. хэш-функция вычисляется быстрее цифровой подписи, то вместо выработки ЭЦП для сообщения, сначала вычисляется его хэш-функция, а уже для значения хэш-функции вырабатывается ЭЦП.

Алгоритм вычисления хэш-функции называют «message digest», а результат вычисления хэш-функции - «цифровым отпечатком пальца» («digital fingerprint»).

См. также Электронная цифровая подпись, Коллизия, Birthday attack.

Хагелина машина

См. С-36

Ц

Целостность

Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

См. также Доступность, Конфиденциальность, Информация.

Цифровая подпись

См. Электронная цифровая подпись.

Цель защиты информации

Предотвращение или минимизация наносимого ущерба (прямого или косвенного, материального, морального или иного) субъектам информационных отношений посредством нежелательного воздействия на компоненты АС, а также разглашения (утечки), искажения (модификации), утраты (снижения степени доступности) или незаконного тиражирования информации.

См. также Защита информации, Субъекты информационных отношений.

Центр распределения ключей

Механизм, позволяющий распределять секретные ключи в симметричных криптосистемах. Существенный недостаток этого механизма заключается в том, что для получения секретного ключа абонента необходимо обратиться в центр распределения ключей (ЦРК) с соответствующим запросом, т.е. ЦРК должен обрабатывать потоки запросов в режиме online (при установлении защищенного соединения каждый абонент-инициатор должен будет обращаться в ЦРК за необходимой ключевой информацией абонента-респондента).

См. также Ключ криптографический, Криптосистема с секретным ключом, Центр сертификации ключей.

Центр сертификации ключей

Механизм, который в отличие от механизма центра распределения ключей, не требует при каждом запросе на установление защищенного соединения, обращаться за ключом абонента-респондента. Данный механизм основан на применении криптосистем с открытым ключом. Перед началом использования открытого ключа абонент, выработавший его, запрашивает в центре сертификации ключей (ЦСК), сертификат, подтверждающий подлинность открытого ключа. При установлении защищенного соединения абоненты обмениваются сертификатами открытых ключей. Перед использованием открытых ключей абоненты могут убедиться в их подлинности путем проверки цифровой подписи сертификата получателя с помощью известного открытого ключа ЦСК.

См. также Ключ криптографический, Криптосистема с открытым ключом, Сертификат, Центр распределения ключей.

См. Digital envelop

Ч

Червь

Программа, распространяющаяся по сети. «Червь» использует уязвимости сетевых протоколов или сетевых программ для распространения своих копий по узлам сети, где он может быть активизирован.

Может быть использован как для санкционированных, так и для несанкционированных действий.

См. также Вирус.

Ш

Шифр

Совокупность обратимых преобразований множества открытых текстов на множество шифртекстов, заданных алгоритмом криптографического преобразования.

См. также Криптографическое преобразование.

Шифрование

См. Криптографическое преобразование

Шифртекст

Результат шифрования открытого текста.

См. также Криптографическое преобразование.

Шарады Меркля

Алгоритм, распределения ключей, разработанный Р. Мерклем. Суть его заключается в том, чтобы передавать используемый для шифрования секретный ключ, скрывая его в большом наборе шарад (головоломки). Каждая шарада содержит криптографический ключ, представляя собой шифртекст, полученный при помощи блочного шифра на малом пространстве ключей. Получив по незащищенному каналу шарады от пользователя А, пользователь В случайным образом выбирает одну из них и решает ее методом полного перебора, зная, что закрытие осуществляется блочным шифром. Вычислив ключ, пользователь В зашифровывает на нем заранее обусловленный текст и пересылает пользователю А в новом наборе шарад. Пользователь А также путем перебора ключей находит ключ, используемый пользователем В и, данный ключ используется для криптографического преобразования сообщений между пользователями А и В.

Стойкость данного метода зависит от числа шарад, составленных пользователем А.

См. также Ключ криптографический, Криптографическое преобразование, Распределение ключей.

Шарады с временным замком

Криптографическая система с временным раскрытием, предложенная Р. Райвестом, А. Шамиром и Д. Вагнером. Сложность решения «шарады» зависит от количества затрачиваемых на решение вычислительных ресурсов. При построении «шарады» основная задача – выбор алгоритма, эффективность которого не зависит от типа его реализации, и решение которого не может быть распараллелено в принципе.

См. также Криптосистема с временным раскрытием, Криптографическая система, Стойкость.

Шифр Фейстеля

Специальный класс повторяющегося блочного шифра, в котором шифртекст вычисляется из открытого текста повторением применения функции обхода. Иногда шифр

Фейстеля называют DES-подобным шифром, т.к. обрабатываемый текст делится на две половины и функция обхода применяется одной половине, используя дополнительный ключ. Результат применения функции обхода затем складывается по модулю 2 (функция XOR) с другой половиной. Затем две половины меняются местами и процесс повторяется.

См. также Iterated Block Cipher, Блочный шифр, Data Encryption Standard.

Шлюз прикладного уровня

См. Application-level Gateway

Шлюз сеансового уровня

См. Circuit-level Gateway

Шлюз двухпортовый

См. Dual-homed Gateway

Шифровальные средства

Реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для защиты информации (в т.ч. и входящие в системы и комплексы защиты информации от несанкционированного доступа), циркулирующей в технических средствах, при ее обработке, хранении и передаче по каналам связи, включая шифровальную технику;

Реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и “электронной подписи”;

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.

См. также Несанкционированный доступ, Криптографическая система, Федеральное агентство правительственной связи и информации.

Э

Экран межсетевой

Является защитным барьером, состоящим из нескольких компонент (например, маршрутизатора или шлюза, на котором работает программное обеспечение межсетевого экрана). Межсетевой экран, также называемый firewall, конфигурируется в соответствии с принятой в организации политикой безопасности. Все входящие и исходящие пакеты должны проходить через межсетевой экран, который пропускает только авторизованные пакеты.

См. также Брандмауэр, Proxy, Packet-filtering firewall, Stateful Inspection firewall, Application-level Gateway.

Экран межсетевой с фильтрацией пакетов

См. Packet-filtering firewall

Электронная цифровая подпись

Механизм, позволяющий на основе криптографических методов надежно установить авторство и подлинность информации (сообщения или документа). Первоначально, поиски эффективных методов генерации электронной цифровой подписи велись на пути использования симметричных криптосистем, в частности алгоритма DES (режим CBC). Однако, для того, чтобы ЭЦП, построенные с применением симметричных криптосистем, удовлетворяли всем, предъявляемым к цифровой подписи, требованиям, необходимы дорогостоящие и трудоемкие организационные меры. Поэтому для реализации механизма электронной цифровой подписи, как правило, применяются криптографические преобразования с открытым ключом.

Электронная цифровая подпись, которая использует открытый ключ, выглядит как обратная системе шифрования с открытым ключом. Если во второй для преобразования (зашифрования) текста используется открытый ключ получателя, то для выработки подписи под конкретным сообщением используется секретный ключ отправителя. Для проверки подписи используется открытый ключ пользователя, который выдает себя за автора сообщения.

На практике, для сокращения времени выработки и проверки цифровой подписи, а также для уменьшения размера подписи, используется общеизвестная функция, действующая на пространстве открытых текстов и отображающая любой открытый текст в сообщение фиксированного малого размера, которое далее и преобразуется в цифровую подпись. Такая функция называется функцией хэширования или хэш-функцией.

См. также Открытое распределение ключей, Односторонняя функция, Криптосистема с открытым ключом, Хэш-функция, Аутентификация.

ЭЦП

См. Электронная цифровая подпись

Экспоненциальное распределение ключей

См. Диффи-Хеллмана алгоритм

Эль-Гамаля алгоритм

Криптосистема, базирующаяся на задаче дискретного логарифмирования. Может использоваться как для шифрования, так и для аутентификации (цифровой подписи) информации. Была предложена в 1985 году Эль Гамалем.

Для генерации пары ключей сначала выбирается простое число p , и два случайных числа g и x , таких, что g и x меньше p . Затем вычисляется

$$y = g^x \bmod p$$

Открытым ключом является тройка чисел (y, g, p) , причем g и p распространяются среди пользователей системы. Число x является секретным ключом.

Для подписи сообщения m сначала выбирается случайное число k , взаимно простое с $p-1$. Затем вычисляется

$$a = g^k \bmod p$$

Затем вычисляется число b :

$$b = k^{-1}(m - xa) \bmod (p - 1)$$

Цифровая подпись сообщения m есть пара чисел (a, b) . Число k должно сохраняться в секрете. Для проверки подписи должно выполняться условие:

$$y^a a^b \bmod p = g^m \bmod p$$

Для зашифрования сообщения m используется формула:

$$b = y^k m \bmod p, \text{ где пара } (a, b) \text{ является шифртекстом}$$

Расшифрование осуществляется по формуле:

$$m = b / a^x \bmod p$$

Схема Эль-Гамаля допускает возможность выработки ложных сообщений и подписей к ним, удовлетворяющих некоторым условиям. Для устранения этого недостатка криптосистема Эль-Гамаля используется только с функцией хэширования открытого текста.

См. также Криптографическая система, Электронная цифровая подпись, Хэш-функция.

Эллиптические кривые

См. Криптосистема с эллиптическими кривыми

Эффективность защиты информации

Степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты.

См. также Показатель эффективности защиты информации

Я

Ядро безопасности

См. Security kernel

A

American National Standards Institute

Американский национальный институт стандартов. Субсидируемая промышленными кругами организация, которая была основана в 1918 г. в США с целью выработки национальных промышленных стандартов и их увязки со стандартами, принятыми ISO.

См. также International Organization for Standardization.

ANSI

См. American National Standards Institute.

ANSI X9.9

Банковский стандарт, также называемый DES-MAC, для аутентификации финансовых транзакций. Базируется на алгоритме DES в режимах CBC и CFB. Более детальный стандарт был опубликован как ANSI X9.19.

Эквивалентные международные стандарты – ISO 8730, ISO 8731 для ANSI X9.9 и ISO 9807 для ANSI X9.19.

См. также American National Standards Institute, Data Encryption Standard, Cipher Block Chaining, Cipher Feedback.

ANSI X9.17

Банковский стандарт, описывающий метод распределения секретных криптографических ключей для симметричных криптосистем на основе алгоритма Triple-DES.

См. также American National Standards Institute, Triple DES.

ANSI X9.23

Банковский стандарт, описывающий алгоритм шифрования DES.

ANSI X9.30

Стандарт, описывающий механизмы криптографического преобразования с открытыми ключами. Состоит из трех частей, в которых описаны алгоритмы DSA, SHA и организационные вопросы, связанные с применением сертификатов для DSA.

См. также American National Standards Institute, Digital Signature Algorithm, SHA.

ANSI X9.31

Стандарт, описывающий механизмы криптографического преобразования с открытыми ключами. Состоит из трех частей, в которых описаны алгоритм электронной цифровой подписи RSA, основанный на действующем стандарте ISO 9796 (первая часть). Во второй части описываются алгоритмы хэширования, используемые с RSA – MD2, MD5, SHA

и MDC-2. В третьей части, аналогичной стандарту X9.30, идет речь об организационных вопросах связанных с применением сертификатов.

См. также American National Standards Institute, RSA, MD2, MD5, SHA.

ANSI X9.41

Стандарт, описывающий протокол согласования атрибутов безопасности между двумя объектами (необходимые услуги, алгоритмы, требования к криптографическим модулям и т.п.).

См. также American National Standards Institute.

ANSI X9.42

Стандарт, описывающий криптографическую процедуру обмена открытыми ключами Диффи-Хеллмана.

См. также American National Standards Institute, Диффи-Хеллмана алгоритм.

ANSI X9.44

Стандарт обмена криптографическими ключами с использованием алгоритма RSA.

См. также American National Standards Institute, Ключ криптографический, RSA.

ANSI X9.45

Стандарт, описывающий усиленные меры контроля на основе сертификатов атрибутов и определяющий направления снижения рисков, связанных с цифровыми подписями.

См. также American National Standards Institute, Электронная цифровая подпись.

ANSI X12.58

Стандарт, устанавливающий структуру безопасности для электронного документооборота (EDI). Описываются функции шифрования, подтверждения подлинности (MAC) и заверения (ЭЦП).

См. также American National Standards Institute, Электронная цифровая подпись, MAC.

Authenticode

Основная технология защиты управляющих элементов ActiveX, разработанная компанией Microsoft. Использует механизм подписи кода.

См. также Подпись кода.

ASSIST

См. Automated Systems Security Incident Support Team

Automated Systems Security Incident Support Team

ASSIST (Automated Systems Security Incident Support Team) был создан для поддержания программы защиты информационных систем Министерства Обороны США (Defense Information Infrastructure, DII) – INFOSEC. Адрес ASSIST: <http://199.211.123.12/>.

См. также CIAC, CERT, FIRST.

Audit

См. Аудит

Audit trail

Журнал, в котором регистрируются события, имеющие отношение к обеспечению безопасности автоматизированной системы. Просмотр данного журнала помогает выявлять попытки несанкционированного доступа к системе и идентифицировать лиц, пытавшихся осуществить такой доступ.

См. также Аудит, Несанкционированный доступ.

Authentication

См. Аутентификация

Access period

Временной интервал, в течение которого действуют права доступа.

См. также Право доступа.

Access control

См. Контроль доступа

Access control list

См. Сборка мусора

Атака, заключающаяся в поиске информации, остающейся в оперативной памяти или на накопителях информации после работы субъекта или объекта системы.

См. также Атака.

Список контроля доступа

Accountability

Свойство автоматизированной системы, позволяющее фиксировать деятельность ее субъектов и ассоциировать их с индивидуальными идентификаторами для установления ответственности за определенные действия.

Assurance

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

См. также Достоверная вычислительная база.

Authorization

См. Авторизация

Asymmetric cryptography

См. Криптосистема с открытым ключом

Adaptive chosen ciphertext attack

Адаптивный метод криптоанализа по выбранным шифртекстам и соответствующим открытым текстам. Данный метод - модификация атаки chosen ciphertext attack. Используется, когда криптоаналитик не только выбирает открытый текст для зашифрования, но также может выбрать этот открытый текст в зависимости от результата предыдущего зашифрования.

См. также Криптоанализ, Chosen ciphertext attack.

Arbitrated protocol

См. Протокол с арбитром

Adjudicated protocol

См. Протокол с третейским судьей

AS2805.6.5.3

Австралийский стандарт управления ключами, основанный на алгоритме RSA.

См. также Управление ключами, RSA.

Application-level Gateway

Один из вариантов реализации межсетевого экрана. Исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Фильтрация всех входящих и исходящих пакетов осуществляется на прикладном уровне эталонной модели OSI. Связанные с приложениями программы-посредники перенаправляют через шлюз информацию, генерируемую конкретными сервисами TCP/IP.

См. также Экран межсетевой, Посредник.

A Guide to Understanding Audit in Trusted Systems

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1, вторая версия которого утверждена 1 июня 1988 года.

Описывает механизмы аудита в автоматизированных системах, обрабатывающих секретную информацию. Документ также известен, как NCSC-TG-001 или Tan Book.

См. также Rainbow series, National Computer Security Center, Аудит.

A Guide to Understanding Discretionary Access Control in Trusted Systems

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный 30 сентября 1987 года. Описывает механизмы дискреционного доступа для использования в автоматизированных системах, которые должны соответствовать TCSEC. Документ также известен, как NCSC-TG-003 или Neon Orange Book.

См. также Rainbow series, National Computer Security Center, Дискреционный доступ, Trusted Computer Security Evaluation Criteria.

A Guide to Understanding Configuration Management in Trusted Systems

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный 28 марта 1988 года. Описывает механизмы управления конфигурацией автоматизированных систем, предназначенных для обработки секретной информации. Документ также известен, как NCSC-TG-006 или Amber Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria.

A Guide to Understanding Design Documentation in Trusted Systems

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный 6 октября 1988 года. Обеспечение разработчиков пониманием требований TCSEC по документированию автоматизированных систем. Документ также известен, как NCSC-TG-007 или Burgundy Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria.

A Guide to Understanding Trusted Distribution in Trusted Systems

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный 15 декабря 1988 года. Определяет механизмы распределения аппаратного и программного обеспечения автоматизированных систем, предназначенных для обработки секретной информации. Документ также известен, как NCSC-TG-008 или Dark Lavender Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria.

A Guide to Understanding Security Modeling in Trusted Systems

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный в октябре 1992 года. Документ предназначен для специалистов, разрабатывающих политику безопасности организации. Документ также известен, как NCSC-TG-010 или Aqua Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria.

A Guide to Understanding Trusted Facility Manuals

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный 18 октября 1989 года. Документ написан в помощь разработчикам защищенных систем, аппаратного обеспечения и конечных пользователей для понимания ими средств «доверенного» управления в классах от B2 до A1 TCSEC. Документ также известен, как NCSC-TG-015 или Brown Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria.

A Guide to Understanding Identification and Authentication in Trusted Systems

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный в сентябре 1991 года. Описывает механизмы идентификации и аутентификации в автоматизированных системах, обрабатывающих секретную информацию. Документ также известен, как NCSC-TG-017 или Light Blue Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria, Аутентификация, Идентификация.

A Guide to Understanding Object Reuse in Trusted Systems

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный в июле 1992 года. Описывает механизмы повторного использования объектов. Документ также известен, как NCSC-TG-018 или Tan Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria, Object reuse.

A Guide to Understanding Trusted Recovery in Trusted Systems

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный 30 декабря 1991 года. Описывает механизмы доверенного восстановления. Документ также известен, как NCSC-TG-022 или Yellow Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria, Recovery procedures.

A Guide to Understanding Security testing and Test Documentation in Trusted Systems

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1. Описывает механизмы тестирования системы защиты и принципы разработки тестовой документации на автоматизированную систему, обрабатывающую секретную информацию. Документ также известен, как NCSC-TG-023 или Bright Orange Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria.

A Guide to Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный в декабре 1992 года. Документ написан в помощь покупателям автоматизированных систем, сертифицированных на соответствие TCSEC. Документ также известен, как NCSC-TG-024 или Purple Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria.

A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work – An Aid to Procurement Initiators

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный в декабре 1992 года. Документ написан в помощь покупателям автоматизированных систем, сертифицированных на соответствие TCSEC. Документ также известен, как NCSC-TG-024 или Purple Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria.

A Guide to Procurement of Trusted Systems: Computer Security Contract Data Requirements List and Data Item Description Tutorial

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный в декабре 1992 года. Документ написан в помощь покупателям автоматизированных систем, сертифицированных на соответствие TCSEC. Документ также известен, как NCSC-TG-024 или Purple Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria.

A Guide to Procurement of Trusted Systems: How to Evaluate a Bidder's Proposal Document – An Aid to Procurement Initiators and Contractors

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный в декабре 1992 года. Документ написан в

помощь покупателям автоматизированных систем, сертифицированных на соответствие TCSEC. Документ также известен, как NCSC-TG-024 или Purple Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria.

A Guide to Understanding Data Remanence in Automated Information Systems

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и вторая версия которого утверждена в сентябре 1991 года. Описывает проблему остаточной памяти и методов ее устранения. Документ также известен, как NCSC-TG-025 или Forest Green Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria, Remanence.

A Guide to Writing the Security Features User's Guide for Trusted Systems

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный в сентябре 1991 года. Описывает принципы создания документации по возможностям защитных механизмов проектируемой автоматизированной системы. Документ также известен, как NCSC-TG-026 или Hot Peach Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria.

A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный в мае 1992 года. Описывает обязанности администратора безопасности по защите информации автоматизированной системы. Документ также известен, как NCSC-TG-027 или Turquoise Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria.

Accessing Controlled Access Protection

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный 25 мая 1992 года. Предназначен для определения, обеспечивает ли автоматизированная система по крайней мере контролируемый доступ к своим ресурсам. Документ также известен, как NCSC-TG-028 или Violet Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria.

A Guide to Understanding Covert Channel Analysis of Trusted Systems

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный в ноябре 1993 года. Определяет механизмы анализа скрытых каналов. Документ также известен, как NCSC-TG-030 или Light Pink Book.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria, Covert channels.

AES

См. Advanced Encryption Standard

Advanced Encryption Standard

Национальный стандарт шифрования США, который "будет определять незасекреченный, т.е. открыто опубликованный алгоритм шифрования, способный защищать важную информацию правительственного уровня" в 21 столетии. Должен быть принят NIST в 1998 году.

Предлагается на замену стандарту DES. Является симметричным блочным шифром, допускающим как программную, так и аппаратную реализацию. Алгоритм оперирует блоками длиной 128 бит, и допускает ключи размеров в 128, 192 и 256 бит.

К концу лета 1999 года должен быть назван один из пятнадцати поданных в NIST алгоритмов.

См. также Data Encryption Standard, RC5, National Institute of Standards and Technology, National Institute of Standards and Technology.

Amber Book

См. A Guide to Understanding Configuration Management in Trusted Systems

Aqua Book

См. A Guide to Understanding Security Modeling in Trusted Systems

В

Blowfish

Блочный шифр, разработанный Брюсом Шнейером (Schneier). Относится к классу шифров Фейстеля. Все операции базируются на операции сложения по модулю 2 (XOR) и дополнении 32-битных слов. Размер блока обрабатываемых данных – 64 бита. Длина ключа – переменная (до 448 бит). Ключ используется для генерации массива дополнительных ключей. Криптосистема разработана специально для использования в 32-разрядных компьютерах и значительно быстрее DES. Несмотря на наличие некоторых уязвимостей и возможность применения дифференциального анализа, на данный момент алгоритм Blowfish считается надежным.

См. также Шифр Фейстеля, Блочный шифр, Data Encryption Standard.

Block Cipher

См. Блочный шифр

Bell-LaPadulla model

См. Белла-Лападулла модель

Backup plan

См. План обеспечения непрерывной работы и восстановления

Banking Circular 226

Документ, опубликованный 25 января 1988 г. Comptroller of the Currency, Administrator of National Bank и одобренный Federal Financial Institutions Examination Council (FFIEC), описывает угрозы, связанные с выполнением вычислений конечными пользователями, и подчеркивает необходимость строго контроля доступа.

BC-226

См. Banking Circular 226

Banking Circular 229

Документ, опубликованный 31 мая 1988 года, предназначен для предупреждения правлений национальных банков США о важности информационной безопасности. Он описывает необходимость защиты всех типов информации, особенно той, которая обрабатывается в автоматизированных системах.

BC-229

См. Banking Circular 229

Blind signature scheme

Механизм электронной цифровой подписи, предложенной известным ученым-криптологом Дэвидом Чомом (David Chaum) в 1994 г. Используется в платежной системе DigiCash и основан на применении случайного множителя (blinding factor).

Пользователь, внося реальные деньги на банковский счет, получает взамен т.н. виртуальные или электронные деньги, которые можно использовать для оплаты покупок в Internet. Электронные деньги представляют собой уникальные последовательности символов, соответствующих каждой монете определенного достоинства.

В основе данной технологии лежит использование криптографии с открытыми ключами. Эмитент электронных денег (банк) кроме пары ключей для своей аутентификации (открытого и закрытого) имеет еще последовательность пар ключей, в соответствие которым ставятся номиналы «цифровых монет».

Для снятия некоторой суммы со своего счета клиент генерирует уникальную последовательность символов, которая затем преобразуется при помощи случайного множителя (blinding factor), неизвестного банку. Затем клиент ставит в соответствие этой преобразованной строке номинал нужной ему монеты. Результат зашифровывается на открытом ключе банка и отсылается в банк. Банк расшифровывает данную строку на своем секретном ключе, заверяет ее электронной подписью, соответствующей номиналу монеты и, после зашифрования ее на открытом ключе клиента, возвращает «монету» обратно, одновременно списывая необходимую сумму со счета клиента.

Клиент, получив «монету», расшифровывает ее на своем секретном ключе. Затем применяя обратное преобразование с blinding factor получает исходный вид «монеты» и помещает ее в свой электронный кошелек (подпись банка при этом остается в целостности и сохранности).

Благодаря «слепой подписи» клиент сохраняет свою конфиденциальность, т.к. банк не может идентифицировать его, не зная blind factor. В то же время банк может отслеживать идентифицировать получателя платежа.

См. также Электронная цифровая подпись.

Brute-force attack

Атака, заключающаяся в поиске пароля из множества всех возможных значений путем его полного перебора.

См. также Атака, Пароль, Brute-force search.

Brute-force 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.

См. также Криптоанализ, Ключ криптографический, Brute-force attack.

Birthday attack

Метод криптоанализа хэш-функции. Относится к классу атак подбора пароля. Атака получила свое название от т.н. «парадокса близнецов», который заключается в вычислении

вероятности того, что два и более членов одной группы родились в один и тот же день. Использует поиск коллизий в хэш-функции.

См. также Хэш-функция, Brute-force search, Криптоанализ, Коллизия.

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.

См. также Stateful Inspection firewall, Экран межсетевой.

Bright Blue Book

См. Trusted Product Evaluations – A Guide for Vendors

Burgundy Book

См. A Guide to Understanding Design Documentation in Trusted Systems

Brown Book

См. A Guide to Understanding Trusted Facility Manuals

Blue Book

1. См. Trusted Product Evaluation Questionnaire
2. См. Introduction to Certification and Accreditation Concepts

Bright Orange Book

См. A Guide to Understanding Security testing and Test Documentation in Trusted Systems

С

Cipher

См. Шифр

Ciphertext

См. Шифртекст

Cipher Block Chaining

Режим сцепления блоков шифра. Для получения нового блока шифртекста каждый блок открытого текста складывается побитно по модулю 2 (функция XOR) с предыдущим блоком шифртекста. Это режим использования блочного шифра является более предпочтительным для шифрования открытого текста и более стойким к атакам криптоаналитиков по сравнению с режимом ECB. Процессы зашифрования и расшифрования, описываются формулами:

$$C_i = E_k(P_i \oplus C_{i-1}), i = 1, 2, \dots$$
$$P_i = C_{i-1} \oplus D_k(C_i), i = 1, 2, \dots$$

Блок шифртекста является функцией только от текущего и предыдущего блоков открытого текста. Поэтому ошибка при передаче приведет при расшифровании к потере только двух блоков исходного текста.

См. также Electronic codebook, Блочный шифр, Data Encryption Standard.

CBC

См. Cipher Block Chaining

Cipher Feedback

Режим обратной связи по шифртексту. В отличие от режима CBC использующего блоки фиксированной длины 64 бит, режим CFB может использовать блоки длиной от 1 до 64 бит. Процессы зашифрования и расшифрования, описывается формулами:

$$C_i = P_i \oplus E_k(C_{i-1}), i = 1, 2, \dots$$
$$P_i = C_i \oplus E_k(C_{i-1}), i = 1, 2, \dots$$

Данный режим использует сдвиговый регистр, на вход которого подаются символы шифртекста, которые образуют вход для функции шифрования. Этот режим использования блочного шифра является примером самосинхронизирующейся потоковой криптосистемы.

См. также Output Feedback, Cipher Block ChainingРегистр сдвига с обратной связью, Блочный шифр, Поточковый шифр.

CFB

См. Cipher Feedback

Capstone

Американский правительственный долгосрочный проект, предназначенный для разработке набора стандартов для криптографии с открытым ключом. Основные организации, ответственные за реализацию проекта – NIST и NSA. Проект состоит из четырех частей:

- алгоритм шифрования данных Skipjack, реализованный в микросхеме Clipper;
- алгоритм цифровой подписи DSA;
- алгоритм хэш-функции SHA;
- протокол обмена ключами. На данный момент данный протокол не опубликован, но из предварительной информации известно, что он основан на схеме Диффи-Хеллмана.

См. также SKIPJACK, SHA, SHS, Digital Signature Standard, Digital Signature Algorithm, Диффи-Хеллмана алгоритм.

Clipper

Микросхема, реализующая алгоритм шифрования Skipjack. Является частью проекта Capstone. Официально объявлено о создании Clipper в апреле 1993 года.

См. также Capstone, SKIPJACK

Code signing

См. Подпись кода

CERT

См. Computer Emergency Response Team

Computer Emergency Response Team

Координационный центр CERT/CC находится в Питсбурге (шт. Пенсильвания, США) при Университете разработки программного обеспечения Карнеги-Мэллона (Carnegie Mellon University's Software Engineering Institute, SEI). SEI, спонсируемый Министерством Обороны США, занимается улучшением методов разработки программного обеспечения. Координационный центр CERT/CC является частью программы, которая разрабатывается в SEI - Networked Systems Survivability (NSS). Основная цель данной программы обеспечить построение соответствующей технологии и методов управления системой таким образом, чтобы максимально эффективно противодействовать атакам, минимизировать ущерб и обеспечить непрерывность работы системы, даже в случае успешного осуществления атаки.

Координационный центр CERT/CC предназначен для решения следующих задач:

- обеспечить постоянную и надежную связь для реагирования на сообщения об атаках;
- обеспечить взаимодействие между экспертами, работающими в области обеспечения информационной безопасности;
- служить центром для идентификации и коррекции уязвимостей в компьютерных системах;
- проводить научные исследования для повышения уровня безопасности существующих систем.

Для периодического ознакомления с обнаруженными в исследовательских лабораториях CERT/CC уязвимостями программного и аппаратного обеспечения на WWW-сервере (<http://www.cert.org>), FTP-сервере (ftp://ftp.cert.org/pub/cert_advisories), в телеконференции USENET (comp.security.announce) и через список рассылки, публикуются т.н. Advisories – описания уязвимостей и способов их устранения. Информация, полученная от фирм-производителей, о проблемах безопасности и их решении публикуется в специальных информационных бюллетенях от поставщиков (Vendor-Initiated Bulletins), распространяемых по тем же каналам, что и Advisories.

См. также ASSIST, CIAC.

CIAC

См. Computer Incident Advisory Capability

Computer Incident Advisory Capability

Центр CIAC (Computer Incident Advisory Capability) был организован при Министерстве Энергетики США в 1989 г. Основной целью CIAC является обеспечение компьютерной безопасности служащих и подрядчиков Министерства Энергетики. CIAC выполняет множество функций, включая:

- обработку сообщений об инцидентах;
- обеспечение компьютерной безопасности служащих и подрядчиков Министерства Энергетики;
- проведение симпозиумов по вопросам информационной безопасности;
- консультации по вопросам защиты информации.

Группа CIAC входит в состав Центра безопасных компьютерных технологий (Computer Security Technology Center, CSTC) и расположена в Lawrence Livermore National Laboratory. Центр CIAC является одним из участников форума FIRST.

Для периодического ознакомления сообщества Internet с «дырами» CIAC аналогично координационному центру CERT/CC публикует информационные бюллетени (Advisories) на своем WWW-сервере (<http://lnl.ciac.gov>) и через список рассылки.

См. также ASSIST, CERT.

Cryptography

См. Криптография

Covert channels

Путь передачи информации, позволяющий двум взаимодействующим процессам обмениваться информацией способом, который нарушает политику безопасности.

См. также Covert storage channel, Covert timing channel.

Covert storage channel

Скрытый канал, обеспечивающий прямую или косвенную запись в пространство памяти одним процессом и чтение этой информации другим процессом. Скрытый канал с памятью обычно связан с использованием ресурсов ограниченного объема, которые разделяются двумя субъектами с различными уровнями безопасности.

См. также Covert timing channel, Covert channels.

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.

См. также Covert channels, Covert timing channel.

Capability

См. Мандат

Confidentiality

См. Конфиденциальность

Contingency plan

См. План обеспечения непрерывной работы и восстановления

Computer Security Agency

Подразделение Министерства Обороны США. Является предшественником NCSC. В августе 1983 года опубликовало отчет Trusted Computer Security Evaluation Criteria.

См. также National Computer Security Center, Trusted Computer Security Evaluation Criteria.

Commercial Product Evaluation

Программа, позволяющая NCSC оценивать коммерческие системы требованиям TCSEC. В случае соответствия реализации системы какому-либо из классов, информация об этом помещается в EPL.

См. также Evaluated Products List, National Computer Security Center, Trusted Computer Security Evaluation Criteria.

Commercial Computer Security Centre

Центр по защите коммерческой информации министерства торговли и промышленности Великобритании (Department of Trade and Industry). Является разработчиком Technical Criteria for Evaluation of Commercial Security Products.

См. также Technical Criteria for Evaluation of Commercial Security Products.

Compromise

См. Компрометация

Counterfeit Access Device and Computer Fraud and Abuse Act of 1984

Федеральный закон США, объявляющий получение несанкционированного доступа к компьютерам федеральных учреждений преступлением.

Computer Fraud and Abuse Act of 1986

Федеральный закон США, объявляющий преднамеренное получение несанкционированного доступа к компьютерам федеральных учреждений и выведение их из строя преступлением.

Computer Security Act of 1987, PL 100-235

Федеральный закон США, ограничивающий вмешательство Министерства Обороны США в деятельность автоматизированных систем федеральных учреждений, не имеющих непосредственного отношения к обороне. Данный документ возлагает защиту грифованной информации на NSA, а разработку требований по обеспечению безопасности негрифованной информации – на NIST.

См. также National Security Agency, National Institute of Standards and Technology.

Computer Misuse Act of 1990

Закон, разработанный в Великобритании и предназначенный для защиты пользователей от несанкционированного доступа к их информации.

Chosen plaintext attack

Метод криптоанализа по выбираемым открытым и соответствующим шифртекстам. Данный метод используется, когда криптоаналитик не только имеет доступ к шифртекстам и соответствующим им открытым текстам, но и также может выбирать открытый текст для зашифрования и дальнейшего анализа.

См. также Криптоанализ, Chosen ciphertext attack, Chosen message attack.

Chosen ciphertext attack

Метод криптоанализа по выбранным шифртекстам и соответствующим открытым текстам. Данный метод используется, когда криптоаналитик может выбирать любой шифртекст и получать доступ к соответствующим им открытым текстам.

См. также Криптоанализ, Chosen plaintext attack, Chosen message attack.

Chosen message attack

Метод криптоанализа по выбранному сообщению. Используется для атак на сообщения с цифровой подписью. Аналогичен методу криптоанализа Chosen ciphertext attack.

См. также Криптоанализ, Chosen plaintext attack, Chosen ciphertext attack.

Ciphertext only attack

Метод криптоанализа по шифртексту. Данный метод используется, когда криптоаналитик имеет в своем распоряжении только несколько шифртекстов, зашифрованных при помощи одного криптографического преобразования.

См. также Криптоанализ, Chosen ciphertext attack, Chosen message attack.

Chosen key attack

Метод криптоанализа по выбранному ключу. Данный метод не подразумевает, что криптоаналитик может выбирать ключи; это означает, что он имеет некоторые предположения о связях между различными ключами. Данный метод на практике не применяется.

См. также Криптоанализ, Chosen ciphertext attack, Chosen message attack.

C-36

Криптографическая роторная машина, также известная как «машина Хагелина», разработанная Арвидом Даммом. C-36 предлагалась фирмой «Криптография» под управлением Бориса Хагелина. Во время второй мировой войны использовалась в американской армии и была известна под названием «M-209 Converter».

См. также Роторная машина

Counter method

См. Счетчиковый метод

Ciphertext auto key

См. Самосинхронизирующаяся потоковая криптосистема

CTAK

См. Ciphertext auto key

Certificate

См. Сертификат

Certificate Revocation List

См. Список аннулированных сертификатов

CAPI

Библиотека процедур и функций для разработчиков, которые могут использовать различные сервисы безопасности и криптографии в прикладном программном обеспечении. Цель применения CAPI – облегчение труда разработчиков и интеграция криптографических

функций в приложения. Также САРІ может использоваться в случае экспортных ограничений на средства криптографической защиты.

Cryptographic application programming interface

См. САРІ

Cryptoki

См. PKCS #11

Circuit-level Gateway

Один из вариантов реализации межсетевого экрана. 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 внешним хостом. После этого шлюз копирует пакеты в обоих направлениях, не осуществляя их фильтрации.

См. также Экран межсетевой.

Challenge-Handshake Authentication Protocol

Протокол аутентификации для протокола соединения по коммутируемым линиям Point-to-Point Protocol (PPP). Протокол определяет трехзвенную схемы «вызов-рукопожатие». Кроме пароля и идентификатора пользователя, в ней также задействуется ключ для их шифрования. Отличительной особенностью схемы является то, что криптографический секретный ключ не передается между проверяемой и проводящей аутентификацию системами.

См. также Password Authentication Protocol, Аутентификация.

CHAP

См. Challenge-Handshake Authentication Protocol

Computer Operations Audit and Security Technology

Цель создания проекта и одноименной лаборатории Computer Operations Audit and Security Technology (COAST):

- исследовательская работа в области информационной безопасности;
- разработка защитных программных и аппаратных средств;
- обучение вопросам обеспечения информационной безопасности.

О создании COAST (<http://www.cs.purdue.edu/coast/>) было официально объявлено в 1992 году. Однако одноименная лаборатория существовала еще задолго до этого. В рамках научно-исследовательских работ, проведенных ее сотрудниками, было опубликовано большое число статей и книг, разработаны такие известные системы, как система анализа защищенности Unix-систем COPS; система контроля целостности файлов Tripwire; система обнаружения атак IDIOT и др.

Проект COAST поддерживается такими крупными компаниями и организациями, как Microsoft, Sun, CISCO, DARPA, AT&T, Internet Security Systems, NSA и многие другие.

COAST

См. Computer Operations Audit and Security Technology

Computer Security Requirements – Guidance for Applying the DoD TCSEC in Specific Environments

Документ, разработанный Центром Компьютерной Безопасности Министерства Обороны США (DoD Computer Security Center) в соответствии с директивой 5215.1 и утвержденный 25 июня 1985 года. Это руководство определяет минимальные требования безопасности к компьютерам Министерства Обороны США на которых обрабатывается секретная информация.

См. также Rainbow series, Trusted Computer Security Evaluation Criteria.

Computer Security Subsystem Interpretation of the TCSEC

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный 16 сентября 1988 года. Расширяет действие документа CSC-STD-001-83.

См. также Rainbow series, National Computer Security Center, Technical Criteria for Evaluation of Commercial Security Products.

CSC-STD-001-83

См. Orange book

CSC-STD-002-85

См. Password Management Guideline

CSC-STD-003-85

См. Computer Security Requirements – Guidance for Applying the DoD TCSEC in Specific Environments

CSC-STD-004-85

См. Technical Rational Behind CSC-STD-003-85: Computer Security Requirements – Guidance for Applying the DoD TCSEC in Specific Environments

D

Digital Signature Algorithm

Алгоритм цифровой подписи, опубликованный Национальным институтом стандартов и технологий США (NIST) в стандарте DSS.

Базируется на проблеме дискретного логарифмирования и происходит от криптосистем Шнора и Эль-Гамала. Может использоваться только для аутентификации. Основное достоинство алгоритма заключается в том, что выработка подписи осуществляется быстрее ее проверки (в отличие от RSA). Длина ключа может составлять до 1024 бит.

Широкого распространения данный алгоритм пока не получил из-за того, что алгоритм был опубликован достаточно недавно и еще не был достаточно исследован, а также из-за секретности при его проектировании.

Является частью проекта Capstone. Опубликован в FIPS PUB 186.

См. также Capstone, Digital Signature Standard, Эль-Гамала алгоритм, RSA.

DSA

См. Digital Signature Algorithm

Digital Signature Standard

Стандарт на электронную цифровую подпись, разработанный NIST и NSA, и опубликованный 19 мая 1994 года. Содержит в себе описание алгоритма DSA. Является частью проекта Capstone. Опубликован в FIPS PUB 186.

См. также Capstone, Digital Signature Algorithm.

DSS

См. Digital Signature Standard.

Diffie-Hellman

См. Диффи-Хеллмана алгоритм.

Data Encryption Standard

Блочная криптосистема, разработанная компанией IBM и признанная в 1977 году американским правительством как официальный стандарт. Размер блока в алгоритме DES – 64 бита, а длина ключа – 56 бит. Является примером шифра Фейстеля с 16-тью циклами. Первоначально был разработан для применения в аппаратуре. Последний раз подтверждался как официальный стандарт в 1993 году.

См. также Шифр Фейстеля, Блочный шифр.

DES

См. Data Encryption Standard.

DESX

Вариант алгоритма DES, предложенный компанией RSA Data Security. DESX использует метод whitening, чтобы скрыть вход и выход алгоритма шифрования. К 56-битному ключу DES добавляется 64-битный ключ, который складывается по модулю 2 (операция XOR) с открытым текстом до первого цикла алгоритма и с результатом работы алгоритма после последнего цикла. Включен в программу защиты электронной почты MailSafe и комплект разработчика компании RSA Data Security - BSAFE.

См. также Data Encryption Standard

Блочная криптосистема, разработанная компанией IBM и признанная в 1997 году американским правительством как официальный стандарт. Размер блока в алгоритме DES – 64 бита, а длина ключа – 56 бит. Является примером шифра Фейстеля с 16-тью циклами. Первоначально был разработан для применения в аппаратуре. Последний раз подтверждался как официальный стандарт в 1993 году.

См. также Шифр Фейстеля, Блочный шифр.

DES.

Disk scavenging

См. **Ошибка! Источник ссылки не найден.**

Denial of service

См. Отказ в обслуживании

Discretionary access control

См. Избирательный доступ

Department of Defense

Министерство обороны США.

DoD

См. Department of Defense

DoD Guidelines for Computer Security

Совокупность правил, установленных Министерством Обороны США для определения степени безопасности узлового программного обеспечения.

См. Rainbow series.

Domain

Уникальный контекст (например, параметры контроля доступа) исполнения программы, множество объектов, к которым субъект может иметь доступ. Имеет иерархическую структуру.

См. также Объект, Субъект.

DAC

См. Discretionary access control

Data security officer

Лицо, отвечающее за обеспечение безопасности обработки данных в системе и за противодействие попыткам неразрешенного использования данных.

См. также Администратор безопасности.

DSO

См. Data security officer

Data Computer Act of 1984

Закон, разработанный в Великобритании и предназначенный для пресечения несанкционированного получения информации. Этот документ требует защиты личных данных от несанкционированного доступа, модификации или разрушения.

Designated Confirmer Signature

Данная схема является балансом между самопроверяющимися цифровыми подписями и доказательство с нулевым знанием. Предложена Чомом в 1994 году. Если в первом случае проверка подлинности сообщения доступна любому абоненту, имеющему открытый ключ подписывающего лица, то во втором – получатель может проверить подлинность сообщения только через взаимодействие с подписывающим лицом. Designated Confirmer подпись позволяет некоторой определенной (designated) стороне подтвердить подлинность (confirm) сообщения без необходимости обращения к подписывающему лицу. В то же время, без помощи подписывающего лица или определенных заранее сторон проверить подлинность сообщения невозможно. Чом разработал реализацию данного вида цифровых подписей с использованием алгоритма RSA.

См. также Электронная цифровая подпись, RSA, Self-authenticating signature scheme.

Differential cryptanalysis

См. Дифференциальный криптоанализ

DES-EEE3

Режим использования алгоритма Triple-DES, в котором три операции шифрования используют три различных ключа.

См. также DES-EDE3, DES-EEE2, DES-EDE2, Triple DES.

DES-EDE3

Режим использования алгоритма Triple-DES, в котором три операции шифрования используют три различных ключа в следующей последовательности зашифрование-расшифрование-зашифрование.

См. также DES-EEE3, DES-EEE2, DES-EDE2, Triple DES.

DES-EEE2

Режим использования алгоритма Triple-DES, в котором первая и третья операции шифрования используют одинаковые ключи. Таким образом, алгоритм использует только два различных ключа.

См. также DES-EEE3, DES-EDE3, DES-EDE2, Triple DES.

DES-EDE2

Режим использования алгоритма Triple-DES, в котором первая и третья операции шифрования используют одинаковые ключи в следующей последовательности зашифрование-расшифрование-зашифрование. Таким образом, алгоритм использует только два различных ключа.

См. также DES-EEE3, DES-EDE3, DES-EEE2, Triple DES.

Digital fingerprint

См. Хэш-функция

Davies-Meyer hash function

Хэш-функция, разработанная Дэвисом и Майером. Базируется на применении алгоритма DES.

См. также Хэш-функция, DES.

Dual-homed Gateway

Компьютер, на котором работает программное обеспечение межсетевого экрана и который имеет две сетевых карты: одна подключена к внутренней сети, а вторая – к внешней. Шлюз передает информацию из одной сети в другую, исключая прямое взаимодействие между ними. К двудомным шлюзам относятся шлюзы сеансового и прикладного уровней.

См. также Экран межсетевой.

Demilitarized zone

Механизм использования межсетевых экранов, для защиты некоторых информационных ресурсов (например, Web-сервера, почтового сервера и т.п.) не только от атак снаружи корпоративной сети, но и от атак изнутри. Для реализации этого механизма, зона, в которой находятся защищаемые ресурсы, ограничивается межсетевыми экранами, т.е.

весь трафик в/из демилитаризованной зоны, исходящий как со стороны внешней сети, так и со стороны внутренней сети.

См. также Экран межсетевой.

DMZ

См. Demilitarized zone

Digital envelop

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.

См. также Криптосистема с секретным ключом, Криптосистема с открытым ключом.

Dark Lavender Book

См. A Guide to Understanding Trusted Distribution in Trusted Systems

E

EIGamal

См. Эль-Гамал алгоритм.

Elliptic Curves

См. Эллиптические кривые.

Electronic codebook

Режим электронной кодовой книги. Работа этого режима использования блочного шифра состоит в криптографическом преобразовании каждого блока текста независимо от остальных блоков с использованием одного криптографического ключа. Основное достоинство – простота реализации, недостаток – недостаточная криптографическая стойкость. Независимое преобразование одинаковых блоков открытого текста приводит к появлению одинаковых блоков шифртекста, что может служить основой для криптоанализа. Процессы зашифрования и расшифрования, описывается формулами:

$$C_i = E_k(P_i), i = 1, 2, \dots$$
$$P_i = D_k(C_i), i = 1, 2, \dots$$

Данный режим соответствует режиму простой замены по ГОСТ 28147-89 и используется для построения функции хэширования по ГОСТ Р 34.11-94.

См. также ГОСТ 28147-89, ГОСТ Р 34.11-94.

ECB

См. Electronic codebook

Evaluated Products List

Список оборудования, аппаратуры и программного обеспечения, которое было оценено и признано соответствующим определенному классу, согласно стандарту "Trusted Computer Security Evaluation Criteria" (TCSEC). EPL включен в "Information System Security Products and Services Catalogue", издаваемый NSA.

См. также Trusted Computer Security Evaluation Criteria.

EPL

См. Evaluated Products List

Electronic Communications Privacy Act of 1986

Федеральный закон США, объявляющий действия лиц, не имеющих полномочий и перехватывающих информацию в телекоммуникационных каналах, преступными.

Enigma

Немецкая криптографическая роторная машина. Использовалась во время второй мировой войны.

См. также Роторная машина

E31.20

Стандарт для подтверждения подлинности информации в сфере здравоохранения США. Частично заимствован из стандарта ANSI X9.30.

См. также ANSI X9.30.

ETEBAC 5

Французский стандарт, использующий алгоритм RSA в банковской индустрии.

См. также RSA.

Exponential key agreement

См. Диффи-Хеллмана алгоритм

Exhaustive key search

См. Brute-force search

Escrowed Encryption Standard

Американский стандарт шифрования с депонированием ключа. Был введен в феврале 1994 года. Стандарт определяет алгоритм Skipjack и метод вычисления специального поля доступа LEAF (Law Enforcement Access Field), позволяющего в последствии раскрывать секретный ключ в целях контроля над соблюдением законности.

См. также Capstone, Clipper, SKIPJACK.

EES

См. Escrowed Encryption Standard

F

Fortezza

PCMCIA-карта, ранее называемая Tessera, разработанная NSA для реализации алгоритмов проекта Capstone.

См. также Capstone.

FEAL

Алгоритм, представленный в 1988 году Шимицу (Shimizu) и Миягучи (Miyaguchi), как альтернативу алгоритму DES. Оригинальная криптосистема, называемая FEAL-4, использует 4 цикла шифрования, ключ и блок размером 64 бита. Однако после того, как была найдена уязвимость были предложено несколько усовершенствований алгоритма – FEAL-8 (с восемью циклами шифрования), FEAL-N (с N циклами шифрования). В 1991 году Бихам и Шамир предложили метод дифференциального криптоанализа для татки на алгоритм с числом циклов шифрования - до 31. В настоящий момент алгоритм FEAL и его модификации не считается достаточно криптостойкими для применения.

См. также Блочный шифр, DES.

Fast Data Encipherment Algorithm

См. FEAL

Flaw

См. Security flaw

Fault

См. Security flaw

Foreign Corrupt Practices Act of 1977

Федеральный закон США, указывает на принятие мер, гарантирующих безопасность и целостность активов всех компаний США, независимо от форм собственности, области деятельности и т.п.

FAPKC

Криптосистема с открытым ключом, использующая теорию конечных автоматов. Разработана китайским криптографом Тао Ренжи (Tao Renji). Было разработано 3 алгоритма FAPKC0, FAPKC1 и FAPKC2. Первый алгоритм использует только линейные компоненты, в то время как второй и третий алгоритмы – один линейный и один нелинейный компоненты каждый.

См. также Криптосистема с открытым ключом.

Fail-stop signature scheme

Схема цифровой подписи, предложенная Ван Хейстом (van Heyst) и Педерсоном (Pederson) для защиты от подделки подписи. Данный вид цифровой подписи является разновидностью одноразовой цифровой подписи. Схема основана на задаче дискретного логарифмирования.

См. также Электронная цифровая подпись, One-time signature.

Firewall

См. Экран межсетевой

Forum of Incident Response and Security Teams

После создания CERT/CC, CIAC и других групп, каждой со своим финансированием, своими целями и требованиями, стало ясно, что без единого, координирующего центра не обойтись. При взаимодействии между группами, зачастую находящимися в разных часовых поясах, возникали языковые и иные проблемы. Поэтому в 1990 году при содействии 11 участников (CERT, CIAC и т.д.) был создан FIRST (Forum of Incident Response and Security Teams) - международный форум, объединяющий практически все группы реагирования на инциденты. К середине 1997 года состав FIRST (<http://www.first.org>) уже насчитывал более 60 команд и групп реагирования на инциденты из различных стран мира.

Цели FIRST:

- Обеспечение сотрудничества между участниками форума для эффективного предотвращения, обнаружения и восстановления информационных систем после компьютерных инцидентов;
- Обеспечение связи между участниками форума для аварийной и консультативной информации о потенциальных угрозах и атаках;
- Облегчение взаимодействия участников FIRST, проводящих исследования в области информационной безопасности;
- Облегчение распределения информации, инструментов и механизмов, обеспечивающих информационную безопасность.

FIRST – организатор ежегодного симпозиума Computer Security Incident Handling Workshop, на котором собираются все команды и группы реагирования на инциденты и на котором они обсуждают свои проблемы. На данном симпозиуме собираются не только участники FIRST, но и все желающие. 2-3 раза в год FIRST организует закрытые коллоквиумы только для своих участников.

Являясь координатором групп реагирования на инциденты, сам форум FIRST не публикует информации о уязвимостях и атаках на компьютерные системы.

См. также ASSIST, CERT, CIAC.

FIRST

См. Forum of Incident Response and Security Teams

Federal Computer Incident Response Capability

FedCIRC (Federal Computer Incident Response Capability) – организация, основанная в конце 1996 г. при участии NIST, CERT и CIAC. Этот центр обеспечивает соответствующей

информацией федеральные невоенные органы власти. Адрес FedCIRC:
<http://csrc.nist.gov/fedcirc/>.

FedCIRC

См. Federal Computer Incident Response Capability

Forest Green Book

См. A Guide to Understanding Data Remanence in Automated Information Systems

G

G-DES

Вариант алгоритма DES предложенный в 1983 году Шаумюллер-Бихлем (Schaumuller-Bichl) для ускорения и усиления алгоритма DES. Ориентирован на блоки большого размера. В 1993 году Бихам и Шамир показали, что стойкость данного алгоритма ниже, чем у алгоритма DES.

См. также DES.

Garbage collecting

См. **Ошибка! Источник ссылки не найден.**

Greedy program

Программы, пытающиеся при выполнении монополизировать системные ресурсы, не давая другим программам возможности его использовать. Программы такого рода приводят к атакам типа “Отказ в обслуживании”.

Green Book

1. «Зеленая книга» - является ответом Германии на Orange Book. Этот документ был предложен в 1990 г. в качестве основы для всевропейской «Белой книги». «Зеленая книга» была одобрена представителями Великобритании, Германии, Франции и Голландии.

В отличие от Orange Book Green Book рассматривает кроме конфиденциальности информации также ее целостность и доступность. Данный документ предназначен не только для военной сферы, но и для коммерческого сектора.

См. также White Book, Orange book.

2. См. Password Management Guideline

Guessed plaintext attack

Метод криптоанализа по предполагаемому открытому тексту. Имея на руках шифртекст, криптоаналитик предполагая, каков был открытый текст, шифрует его на открытом ключе получателя шифртекста. Сравнение полученного шифртекста с фактическим позволяет определить правильным ли было предположение.

См. также Криптоанализ.

Group signature

См. Групповая подпись,

Glossary of Computer Security Terms

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденного 21 октября 1988 года. Содержит термины и определения в области информационной безопасности.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria.

Guidelines for Formal Verification Systems

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденного 1 апреля 1989 года. Определяет правила и методы, которыми необходимо руководствоваться при определении спецификаций и верификации систем, разработанных с учетом требований TCSEC.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria.

Guidelines for Writing Trusted Facility Manuals

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденного в октябре 1992 года. Описывает правила, по которым необходимо создавать руководства по безопасной установке, конфигурации и эксплуатации систем, разработанных с учетом требований TCSEC.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria.

Н

Hash

См. Хэш-функция

Hole

См. Security flaw

Hot Peach Book

См. A Guide to Writing the Security Features User's Guide for Trusted Systems

I

iKP

См. Internet Keyed Payments Protocol.

Internet Keyed Payments Protocol

Протокол для проведения безопасных платежных транзакций между тремя и более сторонами. Разработан в исследовательском центре IBM и научно-исследовательской лаборатории Цюриха. Протокол базируется на криптографии с открытым ключом.

См. также Криптографический протокол.

International Organization for Standardization

Международная организация по стандартизации. Организация, занимающаяся выработкой международных стандартов на самые различные объекты. В т.ч. и в области защиты информации. Основана в 1946 г. и включает в качестве членов более 70 национальных организаций по стандартизации.

См. также American National Standards Institute.

ISO

См. International Organization for Standardization.

IEEE P1363

Рабочая группа ИИЭР, которая занимается разработкой стандартов для криптографии с открытыми ключами, базирующихся на алгоритме RSA, Диффи-Хеллмана и других алгоритмах.

См. также Диффи-Хеллмана алгоритм, RSA.

IEEE 802.10c

Стандарт, описывающий протокол управления ключами. Служит основой для стандарта ANSI X9.41.

См. также ANSI X9.41.

IDEA

См. International Data Encryption Algorithm.

International Data Encryption Algorithm

Это вторая версия блочного шифра, разработанного Лаем (Lai) и Массеем (Massey). Это 64-хбитный повторяющийся блочный шифр с 128-мибитным ключом и 8-мью циклами шифрования. Не относясь к шифрам Фейстеля, в данном алгоритме все же используются

дополнительные ключи, вычисляемые из основного ключа. Данный алгоритм разрабатывался для реализации как в программном, так и в аппаратном обеспечении. Быстродействие – аналогично DES.

Алгоритм IDEA является стойким к линейному и дифференциальному криптоанализу. Имеется 2^{51} слабых ключей.

См. также Блочный шифр, Криптоанализ, DES.

IP-spoofing

Атака, при которой подменяется IP-адрес пакетов, передаваемых по сети. Обычно IP-адрес отправителя (нарушителя) заменяется на адрес, являющийся «доверенным».

Соединение при таком способе атаки возможно с использованием дополнительной услуги протокола IP «источниковая маршрутизация», что позволяет злоумышленнику получать и обрабатывать пакеты, посылаемые объектом атаки, хотя при определенных условиях конфигурации подсети - объекта атаки это не обязательно. В результате блокирование IP-пакетов с источниковой маршрутизацией на брандмауэре может не дать эффекта. Для проведения атак типа IP-обман существуют специальные пакеты, позволяющие «вручную» формировать параметры TCP/IP соединений, подгоняя их формат под разрешенный в системе объекта атаки.

См. также Spoofing.

Identification

См. Идентификация

Information Technology Security Evaluation Criteria

Документ, являющийся европейским стандартом, определяющим требования и процедуры для создания систем повышенной надежности. Одобрен Германией, Францией, Великобританией и Нидерландами и основан на немецком стандарте Green Book.

Все системы могут оцениваться по эффективности (для наиболее защищенных систем) и по функциональности. Данный документ является более развитым по сравнению с Orange Book и Green Book.

См. также Green Book, Trusted Computer Security Evaluation Criteria.

ITSEC

См. Information Technology Security Evaluation Criteria

Internal feedback

См. Output Feedback

Iterated Block Cipher

Повторяющийся блочный шифр, в котором шифрование каждый блок открытого текста осуществляется за несколько циклов. За каждый цикл одно и то же преобразование, также называемое функцией обхода (round function), применяемое к данным, использует

дополнительный ключ. Набор дополнительных ключей обычно вычисляется из секретного ключа пользователя в соответствии с графиком выработки ключей.

Число раундов в повторяющемся шифре зависит от требуемого уровня безопасности. Чем больше число раундов, тем выше защищенность.

См. также Блочный шифр, Шифр Фейстеля, Key schedule.

Intrusion

См. Атака

Intrusion Detection

См. Обнаружение атак

Intrusion Detection System

См. Система обнаружения атак

IPSEC

См. IP Security Protocol

IP Security Protocol

Протокол, разработанный в рамках проекта над защищенной передачей пакетов по протоколу IP (IPv6). Однако теперь этот протокол может применяться и для IPv4. Обмен сеансовыми ключами для шифрования пакетов осуществляется по протоколу ISAKMP/Oakley. В основном, данный протокол предназначен для связи ЛВС через Internet и обычно реализуется аппаратно.

Протокол IPSec определяет два заголовка в составе IP-пакета, используемых системами аутентификации и шифрования: АН (Authentication Header – заголовок аутентификации) и ESP (Encapsulating Security Payload – заголовок протокола безопасного закрытия содержания).

Спецификация IPSec предусматривает два способа применения АН и ESP к IP-пакету. В транспортном режиме аутентификации и шифрованию подвергается только сегмент IP-дейтаграммы, относящийся к транспортному уровню. А в режиме туннелирования, обеспечивающего более высокий уровень защиты, чем транспортный режим, аутентификация и шифрование распространяются на весь пакет.

Механизм аутентификации в спецификации IPSec не описан.

См. также Internet Security Association & Key Management Protocol

Структура, предназначенная для управления ключами в сети Internet. Самостоятельно не позволяет обмениваться сеансовыми ключами, но в совокупности с другими протоколами, например, Oakley, обеспечивает надежное решение по управлению ключами в Internet.

См. также Oakley.

ISAKMP

См. Internet Security Association & Key Management Protocol.

Layer 2 Forwarding, Layer 2 Tunneling Protocol, Point-to-Point Tunneling Protocol, Virtual Private Network.

Integrity

См. Целостность

Introduction to Certification and Accreditation Concepts

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденного в январе 1994 года. Описывает некоторые понятия в области сертификации и аккредитации.

См. также Rainbow series, National Computer Security Center, Trusted Computer Security Evaluation Criteria, Аккредитация, Сертификация СЗИ.

Internet Security Association & Key Management Protocol

Структура, предназначенная для управления ключами в сети Internet. Самостоятельно не позволяет обмениваться сеансовыми ключами, но в совокупности с другими протоколами, например, Oakley, обеспечивает надежное решение по управлению ключами в Internet.

См. также Oakley.

ISAKMP

См. Internet Security Association & Key Management Protocol.

IKE

См. Internet Key Exchange

Internet Key Exchange

Протокол управления ключами ISAKMP/Oakley.

См. также ISAKMP, Oakley.

К

Knapsack

Kerberos

Схема аутентификации, разработанная в Массачусетском техническом институте. Основана на публикации Нидхема (Needham) и Шредера (Schroeder), опубликованной в 1978 году. Первая доступная для использования версия имела номер 4. Текущая, пятая, версия устранила некоторые недостатки предыдущей версии и была опубликована в 1994 году. Для шифрования и аутентификации используется криптосистемы с секретным ключом. Основное предназначение Kerberos аутентификация запросов к сетевым ресурсам, аутентификации документов не производится.

См. также Аутентификация.

Known plaintext attack

Метод криптоанализа по известному открытому тексту. Данный метод используется, когда криптоаналитик имеет доступ к шифртекстам и соответствующим им открытым текстам.

См. также Криптоанализ.

Key

См. Ключ криптографический

Key stream generator

См. Генератор ключевого потока

Key auto key

См. Синхронизирующаяся потоковая криптосистема

КАК

См. Key auto key

Key schedule

Множество дополнительных ключей для криптографического преобразования, вычисленных из секретного ключа.

См. также Ключ криптографический, Секретный ключ.

Key management

См. Управление ключами

Key generation

Процесс генерации криптографических ключей. Согласно правилу Киркоффа, 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.

См. также Правило Киркоффа, Ключ криптографический, Стойкость.

Key distribution

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.

См. также Ключевая система, Центр распределения ключей, Открытое распределение ключей.

Key storage

Процесс хранения ключей.

Key deletion

Процесс удаления ключей.

Key recovery

Процесс восстановления ключей.

Key crunching

Метод преобразования легко запоминающихся и осмысленных фраз в псевдослучайный ключ с помощью какой-либо процедуры, например, хэш-функции.

См. также Ключ криптографический, Хэш-функция.

Key escrow

Процесс депонирования ключей, заключающийся в разбиении криптографического ключа на две части, каждая из которых шифруется и передается на хранение доверенным агентам депозитной службы. Агенты представляют собой правительственные организации,

обеспечивающие надежное хранение ключевых компонент в течении срока их действия. Агенты выдают их только тогда, когда соответствующий запрос подтвержден решением Федерального Суда США. Полученные компоненты позволяют службам, отвечающим за национальную безопасность, восстановить уникальный ключ и выполнить расшифрование сообщения.

См. также Escrowed Encryption Standard.

L

LUC

Криптосистема, разработанная группой австралийских и новозеландских исследователей. Различные криптографы разработали обобщения алгоритма RSA, которые используют различные перестановки многочленов вместо возведения в степень. Одна из таких систем – LUC, которая использует последовательности Лукаса (Lucas sequences).

См. также Криптографическая система, RSA.

Least privilege

См. Минимум привилегий

Link encryption

См. Канальное шифрование

Loophole

См. Security flaw

Label

См. Метка

Linear Feedback Shift Register

См. Регистр сдвига с обратной связью

LFSR

См. Linear Feedback Shift Register

Layer 2 Forwarding

Протокол для создания VPN. Разработан при значительном участии компании Cisco Systems. Основное отличие от протокола PPTP – необязательное использование сетей, функционирующих по протоколу IP. Протокол L2F позволяет создавать защищенные туннели в сетях протоколов Frame Relay или ATM. Другим отличием от протокола PPTP является поддержка нескольких одновременных соединений. Для аутентификации используются протоколы PAP, TACACS+ и RADIUS.

См. также IP Security Protocol, Layer 2 Tunneling Protocol, Remote Authentication Dial-in User Service, Password Authentication Protocol, TACACS+, Virtual Private Network, Point-to-Point Tunneling Protocol, IP Security Protocol.

L2F

См. Layer 2 Forwarding

Layer 2 Tunneling Protocol

Протокол для создания VPN. В настоящий момент разрабатывается IETF для устранения недостатков протоколов PPTP и L2F. В основном, предназначен для организации удаленного доступа к ресурсам сети (например, для мобильных пользователей). Использует протокол PAP для аутентификации. Для усиления криптозащиты используются элементы протокола IPSec. В настоящий момент работает в IP-сетях, но ведутся разработки для совместимости с сетями X.25, ATM и Frame Relay.

См. также IP Security Protocol, Layer 2 Forwarding, Password Authentication Protocol, Virtual Private Network, Point-to-Point Tunneling Protocol, IP Security Protocol.

L2TP

См. Layer 2 Tunneling Protocol

Light Yellow Book

См. Computer Security Requirements – Guidance for Applying the DoD TCSEC in Specific Environments.

Light Blue Book

1. См. A Guide to Understanding Identification and Authentication in Trusted Systems
2. См. A Guide to Understanding Object Reuse in Trusted Systems

Light Pink Book

См. A Guide to Understanding Covert Channel Analysis of Trusted Systems

М

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.

См. также Одноразовая цифровая подпись, Хэш-функция.

McEliece cryptosystem

См. Криптосистема МакЭлиса.

MIME Object Security Service

Стандарт для защиты почтовых сообщений в формате MIME. Определен в RFC 1847 – 1848. Данный стандарт поддерживает следующие услуги безопасности:

- шифрование;
- электронная цифровая подпись.

Для шифрования сообщений используется алгоритм DES в режиме CBC, для шифрования криптографических ключей – RSA. Электронная цифровая подпись соответствует алгоритму RSA, хэш-функции – MD2 и MD5. Сертификаты соответствуют стандарту X.509.

Недостатком MOSS является тот факт, что, хотя он и является стандартом Internet, он не нашел такого распространения как PEM. Кроме того, число поддерживаемых криптографических алгоритмов мало.

См. также PEM, CBC, MD2, MD5, RSA.

MOSS

См. MIME Object Security Service

MAC

1. См. Mandatory access control
2. См. Message Authentication Code.

MD2

Алгоритм хэш-функции, разработанный Райвестом в 1989 году. Вырабатывает 128-битное значение хэш-функции. Ориентирован на 8-рядные компьютеры. Подробное описание можно найти в RFC 1319. Защищаемое сообщение, дополняется так, чтобы его длина была кратна 16. Затем 16-байтовая контрольная сумма добавляется к сообщению и от полученного результата вычисляется хэш-функция.

См. также Хэш-функция, MD4, MD5.

MD4

Алгоритм хэш-функции, разработанный Райвестом в 1990 году. Вырабатывает 128-битное значение хэш-функции. Ориентирован на 32-рядные компьютеры. Подробное описание можно найти в RFC 1320. Защищаемое сообщение, дополняется так, чтобы его длина плюс 448 бит была кратна 512. Затем 64-битовое двоичное представление оригинальной длины сообщения конкатенируется с самим сообщением и от полученного результата вычисляется хэш-функция. В 1995 были найдены методы криптоанализа, позволяющие определить коллизии для хэш-функции в течении нескольких минут на типичном персональном компьютере.

См. также Хэш-функция, MD5, MD2.

MD5

Алгоритм хэш-функции, разработанный Райвестом в 1991 году. Вырабатывает 128-битное значение хэш-функции. Ориентирован на 32-рядные компьютеры. Подробное описание можно найти в RFC 1321. Это модификация алгоритма MD4, более безопасная, но и более медленная.

См. также Хэш-функция, MD4, MD2.

Masquerade

См. Маскарад

Mandatory access control

См. Мандатный доступ

Multilevel security

Класс систем, содержащих информацию с различными уровнями критичности, которые разрешают одновременный доступ к объектам субъектам с различными уровнями прозрачности, но запрещают при этом несанкционированный доступ.

См. также Многоуровневая защита

M-209 Converter

См. С-36

Message Authentication Code

Механизм, предназначенный для защиты сообщения от модификации и навязывания ложных данных. Может базироваться на механизме одноразового блокнота, хэш-функций, потоковых или блочных шифрах.

Стинсон (Stinson) и Симмонс (Simmons) в 1995 году предложили схему, базирующуюся на использовании одноразового блокнота. Шифртекст аутентифицирует сам себя, т.к. доступ к секретному ключу ограничен.

Когда код аутентификации сообщения базируется на односторонних хэш-функциях, отличием от них является наличие секретного ключа. Только абонент, имеющий секретный ключ может проверить значение хэш-функции.

Лай, Рюппель (Rueppel) и Вульвен (Woolven) предложили схему, основанную на потоковой криптосистеме. Открытый текст разбивается на два потока, которые подаются на вход регистрового сдвига с обратной связью. Конечное состояние двух регистровых сдвигов и есть MAC.

Использование блочных шифров, как правило, основано на применении режима сцепления блоков (CBC). Последний блок шифртекста и является кодом подтверждения подлинности сообщения.

См. также Имитозащита, Имитовставка, Блочный шифр, Потоковый шифр, Хэш-функция.

Message integrity check

См. Имитовставка.

Message Security Protocol

Протокол безопасности сообщений, разработанный Министерством Обороны США и предназначенный для использования в системе оборонных сообщений (Defense Message System, DMS). Он описывает пакет безопасности для сообщения типа X.400. В число поддерживаемых функций безопасности входят подтверждение подлинности, целостность (на основе алгоритма DSS), шифрование (на основе алгоритма Skipjack) и обмен ключами (на основе проекта Capstone).

См. также Capstone, DSS, SKIPJACK.

MSP

См. Message Security Protocol

Man-in-the-middle

Атака, которая заключается в том, что нарушитель вмешивается в процесс обмена ключами между пользователями системы. Получив открытый ключ от пользователя А нарушитель заменяет его на свой открытый ключ и отправляет пользователю В. Аналогично, нарушитель подменяет открытый ключ пользователя В. Таким образом, нарушитель может расшифровывать все сообщения, посылаемые пользователями А и В, модифицировать их и перезашифровывать перед дальнейшей отправкой истинному получателю.

Middleperson attack

См. Man-in-the-middle

Message Digest

См. Хэш-функция

N

National Institute of Standards and Technology

Американский институт по стандартам и технологии, являющийся отделением Министерства Торговли. Ранее было известно как Национальное Бюро Стандартов. В 1987 году согласно Computer Security Act был уполномочен для разработки стандартов в области безопасности. Опубликовал много стандартов в области защиты информации, в т.ч. и разработанные другими группами по стандартизации. В основном, эти стандарты предназначены для федерального правительства. Все официальные стандарты публикуются в т.н. публикациях FIPS (FIPS PUB).

NIST

См. National Institute of Standards and Technology

NBS

См. National Institute of Standards and Technology

National Security Agency

Агентство национальной безопасности США. Было создано Гарри Трумэном в 1952 году. Является аналогом Федерального Агентства Правительственной Связи и Информации при Президенте России. Участвовало в разработке многих криптографических стандартов.

См. также Федеральное агентство правительственной связи и информации.

NSA

См. National Security Agency

NASIRC

См. NASA Automated Systems Incident Response Capability

NASA Automated Systems Incident Response Capability

Центр NASA Automated Systems Incident Response Capability (NASIRC) был создан американским аэрокосмическим агентством (NASA) для выполнения инструкции OMB A-130, закона Computer Security Act от 1987 года и других федеральных законов, нормативных документов и правил, имеющих отношение к защите информационных технологий.

Центр NASIRC (<http://www-nasirc.nasa.gov>) координирует, управляет и обеспечивает технической поддержкой по вопросам информационной безопасности, включая реагирование на атаки, все подразделения NASA. NASIRC решает следующие задачи:

- Анализ, координация деятельности и реагирование на широкий диапазон атак и угроз компьютерам и сетям. Исследование и выработка способов и рекомендаций, уменьшающих риск информационным системам.

- Анализ имеющихся на рынке средств защиты и распределение их среди подразделений NASA;
- Обучение служащих NASA. Выпуск брошюр и информационных бюллетеней, повышающих осведомленность пользователей в области защиты информации.

Аналогично многим другим командам реагирования на атаки, NASIRC входит в FIRST. NASIRC выполняет свои функции путем сотрудничества и координации внутренних подгрупп реагирования на инциденты, а также взаимодействуя с внешними организациями, типа FIRST.

National Computer Security Center

Национальный центр компьютерной безопасности - организация, поддерживающая и стимулирующая распространение защищенных систем в учреждениях Федерального правительства. Являясь подразделением Агентства национальной безопасности, во меж время осуществляет координацию в области анализа и разработки систем с гарантированной защитой. Первичное название - Агентство Компьютерной Безопасности (Computer Security Agency) министерства обороны США (DoD Computer Security Center).

NCSC

См. National Computer Security Center

Nonrepudiation

Невозможность отказа от факта получения или отправления сообщения.

New Directions in Cryptography

Публикация Диффи и Хеллмана, описывающая протокол открытого распределения ключей. Появилась в 1976 году.

См. также Диффи-Хеллмана алгоритм, Открытое распределение ключей.

Niederreiter cryptosystem

См. Криптосистема Нидеррайтера

NCSC-TG-001

См. A Guide to Understanding Audit in Trusted Systems

NCSC-TG-002

См. Trusted Product Evaluations – A Guide for Vendors

NCSC-TG-003

См. A Guide to Understanding Discretionary Access Control in Trusted Systems

См. Glossary of Computer Security Terms	NCSC-TG-004
См. The Trusted Network Interpretation of Department of Defense Trusted Computer System Evaluation Guidelines	NCSC-TG-005
См. A Guide to Understanding Configuration Management in Trusted Systems	NCSC-TG-006
См. A Guide to Understanding Design Documentation in Trusted Systems	NCSC-TG-007
См. A Guide to Understanding Trusted Distribution in Trusted Systems	NCSC-TG-008
См. Computer Security Subsystem Interpretation of the TCSEC	NCSC-TG-009
См. A Guide to Understanding Security Modeling in Trusted Systems	NCSC-TG-010
См. Trusted Network Environments Guideline – Guidance for Applying the TNI	NCSC-TG-011
См. RAMP Program Document	NCSC-TG-013
См. Guidelines for Formal Verification Systems	NCSC-TG-014
См. A Guide to Understanding Trusted Facility Manuals	NCSC-TG-015
См. Guidelines for Writing Trusted Facility Manuals	NCSC-TG-016

NCSC-TG-017

См. A Guide to Understanding Identification and Authentication in Trusted Systems

NCSC-TG-018

См. A Guide to Understanding Object Reuse in Trusted Systems

NCSC-TG-019

См. Trusted Product Evaluation Questionnaire

NCSC-TG-020

См. Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX[®] System

NCSC-TG-021

См. Trusted Database Management System Interpretation of the TCSEC

NCSC-TG-022

A Guide to Understanding Trusted Recovery in Trusted Systems

NCSC-TG-023

См. A Guide to Understanding Security testing and Test Documentation in Trusted Systems

NCSC-TG-024

См. A Guide to Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements, A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work – An Aid to Procurement Initiators, A Guide to Procurement of Trusted Systems: Computer Security Contract Data Requirements List and Data Item Description Tutorial, A Guide to Procurement of Trusted Systems: How to Evaluate a Bidder's Proposal Document – An Aid to Procurement Initiators and Contractors

NCSC-TG-025

См. A Guide to Understanding Data Remanence in Automated Information Systems

NCSC-TG-026

См. A Guide to Writing the Security Features User's Guide for Trusted Systems

NCSC-TG-027

См. A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems

NCSC-TG-028

См. Accessing Controlled Access Protection

NCSC-TG-029

См. Introduction to Certification and Accreditation Concepts

NCSC-TG-030

См. A Guide to Understanding Covert Channel Analysis of Trusted Systems

Neon Orange Book

См. A Guide to Understanding Discretionary Access Control in Trusted Systems

О

One-time pad

См. Одноразовый блокнот

Output Feedback

Режим обратной связи по выходу. Это режим использования блочного шифра также как и режим CFB использует переменный размер блока и сдвиговый регистр. Процессы зашифрования и расшифрования, описываются формулами:

$$C_i = P_i \oplus S_i; S_i = E_k(C_{i-1}), i = 1, 2, \dots$$

$$P_i = C_i \oplus S_i; S_i = E_k(C_{i-1}), i = 1, 2, \dots$$

Отличием от режима CFB состоит в методе обновления сдвигового регистра. Этот режим также называют режимом внутренней связи по выходу (internal feedback). Этот режим использования блочного шифра является примером синхронизирующейся потоковой криптосистемы.

См. также Cipher Feedback, Счетчиковый метод, Блочный шифр, Регистр сдвига с обратной связью, Поточковый шифр, Синхронизирующаяся потоковая криптосистема.

OFB

См. Output Feedback

Object Signing

Механизм подписи кода, используемый в продуктах компании Netscape. Аналогичен технологии Authenticode. Позволяет подписывать апплеты Java и сценарии JavaScript.

См. также Authenticode, Подпись кода.

Orange book

См. Trusted Computer Security Evaluation Criteria.

Object

См. Объект

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.

ОМВА-123

Директива федерального правительства США, определяющая, что при выполнении любыми правительственными органами или любыми компаниями работ для правительства с использованием компьютеров подрядчики должны составить краткий план защиты ресурсов их информационной системы.

Opus novum

Вторая из известных книг по криптологии. Издана в 1526 году в Риме Джакомо Сильвестри.

См. также Polygraphia.

One-way function

См. Односторонняя функция.

One-time signature

См. Одноразовая цифровая подпись.

Oakley

Протокол обмена ключами, основанный на алгоритме Диффи-Хеллмана. Предназначен для установки ключей на хосты и маршрутизаторы Internet. Как правило, используется вместе с ISAKMP. Однако в этом случае депонирование ключей невозможно.

См. также Диффи-Хеллмана алгоритм, Депонирование ключей, ISAKMP.

Р

PKCS

См. Public-Key Cryptography Standards.

PKCS #1

Определяет механизмы для шифрования и подписи информации, используя алгоритм RSA.

См. также RSA.

PKCS #3

Определяет механизмы распределения ключей, используя алгоритм Диффи-Хеллмана.

См. также Диффи-Хеллмана алгоритм.

PKCS #5

Описывает методы шифрования строки данных на секретном ключе, определенном из пароля.

PKCS #6

Описывает формат для расширенных сертификатов. Расширение включает дополнительные по отношению к стандарту X.509 атрибуты. Однако данный стандарт похож на версию 3 стандарта X.509.

См. также X.509.

PKCS #7

Определяет общий формат сообщений, которые включают криптографические расширения типа цифровых подписей и шифрования.

См. также Шифрование, Электронная цифровая подпись.

PKCS #8

Описывает формат информации о секретном ключе в криптосистеме с открытым ключом. Формат включает секретный ключ и набор дополнительных атрибутов.

См. также Криптосистема с открытым ключом.

PKCS #9

Определяет типы атрибутов для других PKCS.

PKCS #10

Описывает формат запроса на сертификацию открытого ключа.
См. также Открытый ключ, Сертификат.

PKCS #11

Определяет программный интерфейс, называемый Cryptoki, независимый от технологии для криптографических устройств типа смарт-карт и PCMCIA-карт (например, Fortezza).

См. также Fortezza.

Public-Key Cryptography Standards

Набор стандартов для криптографии с открытым ключом, разработанный компанией RSA Data Security совместно с неформальным консорциумом, который первоначально включал в себя Apple, Microsoft, DEC, Lotus, Sun и MIT. В настоящий момент опубликованы стандарты #1, #3, #5, #6, #7, #8, #9, #10 и #11.

PKCS определяют как алгоритмо-зависимые, так и алгоритмо-независимые реализации. Поддерживаются многие алгоритмы, однако детально описаны лишь алгоритмы Диффи-Хеллмана и RSA. Данные стандарты периодически пересматриваются и дополняются с учетом последних достижений в области криптографии.

См. также PKCS #1, PKCS #3, PKCS #5, PKCS #6, PKCS #7, PKCS #8, PKCS #9, PKCS #10, PKCS #11.

Public key

См. Открытый ключ

Private key

См. Секретный ключ

Privacy Enhanced Mail

Стандарт защиты почтовых сообщений в Internet. Обеспечивает шифрование и цифровую подпись сообщений. Описание данного стандарта содержится в RFC 1421 – 1424.

В PEM реализованы следующие варианты применения механизмов безопасности:

- Подпись сообщения;
- Шифрование и подпись сообщения.

Каждое PEM-сообщение содержит ЭЦП отправителя. Не подписанные сообщения не поддерживаются.

Для шифрования сообщений используется алгоритм DES в режиме CBC, для шифрования криптографических ключей – RSA (для открытого распределения ключей) или DES в режиме CBC или TripleDES (для симметричного распределения ключей). Электронная цифровая подпись соответствует алгоритму RSA, хэш-функции – MD2 и MD5. Сертификаты соответствуют стандарту X.509.

См. также MIME Object Security Service, DES, RSA, Triple DES, X.509, MD2, MD5.

PEM

См. Privacy Enhanced Mail

PEM-MIME

См. MOSS

PCT

См. Private Communication Technology

Private Communication Technology

Протокол для установления защищенного соединения, разработанный компанией Microsoft. Протокол PCT обладает обратной совместимостью с SSL 2.0. Т.к. PCT очень тесно завязан на SSL, то при создании систем на базе PCT разработчики обязаны покупать лицензию на использование SSL.

См. также SSL.

Point-to-Point Tunneling Protocol

Протокол для создания VPN, разработанный фирмой Ascend Communications, компанией Microsoft и рядом других производителей. В основном, предназначен для организации удаленного доступа к ресурсам сети (например, для мобильных пользователей). Данный протокол встроен в продукты компании Microsoft, в частности операционные системы Windows NT и Windows 98. Протокол PPTP не поддерживает мощных средств шифрования и схем аутентификации пользователей при помощи генераторов паролей. Для аутентификации используются протокол PAP.

См. также IP Security Protocol, Layer 2 Forwarding, Layer 2 Tunneling Protocol, Virtual Private Network, Password Authentication Protocol.

PPTP

См. Point-to-Point Tunneling Protocol

Principal

1. Объект, который может быть аутентифицирован.
2. Инициатор, который может инициировать взаимодействие с объектом системы и при этом не выступать от имени другого объекта. Принципалом может быть любой пользователь системы или активный объект системы.

Preferred Products List

Список коммерческой продукции (аппаратуры и оборудования), прошедшей испытания по программе TEMPEST и удовлетворяющей другим требованиям NSA. PPL включен в «Information System Security Products and Services Catalogue», издаваемый NSA.

См. также Evaluated Products List, TEMPEST.

PPL

См. Preferred Products List

Process

Выполняющаяся программа.

См. также Domain, Субъект.

Protocol

Набор правил и форматов, семантических и синтаксических, позволяющих различным компонентам системы обмениваться информацией (например, узлам сети).

Plaintext

См. Открытый текст

Public-key cryptography

См. Криптосистема с открытым ключом

Privacy Act of 1974

Федеральный закон США, требующий от федеральных учреждений придерживаться определенных правил хранения документов и передачи внутренней информации. Относится только к федеральным системам обработки данных.

Также позволяет гражданам США контролировать и вносить изменения в записи, хранящиеся в правительственных учреждениях.

Purchase key attack

См. Rubber hose cryptanalysis

Purple

Японская криптографическая роторная машина. Использовалась во время второй мировой войны.

См. также Роторная машина

Polygraphia

Первая книга по криптологии, выпущенная в 1518 году в германском городе Рейне. Ее автор - аббат Йоханес Тритемиус.

См. также Opus novum.

Propagating Cipher Block Chaining

Режим сцепления блоков шифра с распространением, аналогичный режиму CBC. Процессы зашифрования и расшифрования, описываются формулами:

$$C_i = E_k(P_i \oplus C_{i-1} \oplus P_{i-1}), i = 1, 2, \dots$$
$$P_i = C_{i-1} \oplus P_{i-1} \oplus D_k(C_i), i = 1, 2, \dots$$

См. также Блочный шифр, Cipher Block Chaining.

PCBC

См. Propagating Cipher Block Chaining

Plaintext Block Chaining

Режим сцепления блоков открытого текста, аналогичный режиму CBC. Процессы зашифрования и расшифрования описываются формулами:

$$C_i = E_k(P_i \oplus P_{i-1}), i = 1, 2, \dots$$
$$P_i = P_{i-1} \oplus D_k(C_i), i = 1, 2, \dots$$

См. также Блочный шифр, Cipher Block Chaining.

PBC

См. Plaintext Block Chaining

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.).

См. также Экран межсетевой.

Proxy

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 каналные посредники, которые обеспечивают те же функции перенаправления запросов, но поддерживают большую часть сервисов TCP/IP.

См. также Экран межсетевой.

Proxy Server

Межсетевой экран, в котором используется механизм трансляции адресов (network address translation) для преобразования IP-адресов всех авторизованных клиентов в IP-адрес, ассоциированный с межсетевым экраном. Работает на сетевом уровне модели OSI.

См. также Экран межсетевой, Проxy.

Password Authentication Protocol

Протокол аутентификации для протокола соединения по коммутируемым линиям Point-to-Point Protocol (PPP). Протокол предусматривает пересылку незашифрованного пароля и идентификатора пользователя. Компьютер, иницирующий процесс аутентификации, посылает их до тех пор, пока система, проводящая аутентификацию, не подтвердит подлинность пользователя или не разорвет соединение.

См. также Challenge-Handshake Authentication Protocol, Аутентификация.

PAP

См. Password Authentication Protocol

Personal Information Exchange

Стандарт, предложенный компаний Microsoft и определяющий способ хранения личной секретной информации и переноса ее с одного пользовательского компьютера на другой.

PFX

См. Personal Information Exchange

Partial Key Escrow

Механизм, предложенный А. Шамиром для устранения недостатков метода депонирования ключей. Данный механизм предполагает передачу на хранение не самого секретного ключа, а его части. При этом для раскрытия секретного ключа необходимо выполнить перебор в объеме, необходимом для восстановления недостающей части.

См. также Escrowed Encryption Standard, Key escrow.

Password Management Guideline

Документ, разработанный Центром Компьютерной Безопасности Министерства Обороны США (DoD Computer Security Center) в соответствии с директивой 5215.1 и утвержденный 12 апреля 1985 года. Описывает принципы аутентификации, основанные на механизме паролей.

См. также Rainbow series, Пароль, Аутентификация.

Pink Book

См. RAMP Program Document

Purple Book

1. См. Guidelines for Formal Verification Systems
2. См. Trusted Database Management System Interpretation of the TCSEC
3. См. A Guide to Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements
4. См. A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work – An Aid to Procurement Initiators
5. См. A Guide to Procurement of Trusted Systems: Computer Security Contract Data Requirements List and Data Item Description Tutorial
6. См. A Guide to Procurement of Trusted Systems: How to Evaluate a Bidder’s Proposal Document – An Aid to Procurement Initiators and Contractors

Q

Quantum cryptography

См. Квантовая криптография

R

RSA

Криптосистема с открытым ключом, используемая как для шифрования, так и для аутентификации (цифровой подписи) информации. Была предложена в 1977 году американскими учеными Роном Райвестом (Ron Rivest), Ади Шамиром (Adi Shamir) и Леонардом Адлеманом (Leonard Adleman), по первым буквам фамилий которых она и названа. Криптосистема RSA базируется на сложности факторизации больших чисел. В качестве открытого и секретного ключей используются простые числа не менее 200 разрядов. Алгоритм RSA работает следующим образом:

1. Выбираются два больших простых числа p и q , желательно эквивалентной длины.
2. Вычисляется число n , равное произведению p и q .
3. Выбираем ключ шифрования e , такое что e и произведение $(p-1)(q-1)$ являются взаимно простыми. Совокупность (e, n) является открытым ключом шифрования.
4. Вычисляем ключ расшифрования d , такое, что:

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

Совокупность (d, n) является секретным ключом шифрования.

5. Для зашифрования сообщения m используется формула:

$$c = m^e \pmod n, \text{ где } (e, n) - \text{открытый ключ получателя сообщения}$$

6. Для расшифрования сообщения c используется формула:

$$m = c^d \pmod n, \text{ где } (d, n) - \text{секретный ключ получателя сообщения}$$

7. Числа p и q после вычисления секретного ключа d уничтожаются:
8. Для выработки цифровой подписи сообщения m используется формула:

$$s = m^d \pmod n, \text{ где } (d, n) - \text{секретный ключ отправителя сообщения}$$

9. Для проверки цифровой подписи сообщения m используется формула:

$$m = s^e \pmod n, \text{ где } (e, n) - \text{открытый ключ отправителя сообщения}$$

Криптосистема RSA является частью многих мировых стандартов. Например, ISO 9796, ITU-T X.509, ETEBAC 5, ANSI X9.31, SWIFT, AS2805.6.5.3 и многих других. Алгоритм RSA запатентован 29 сентября 1983 компанией RSA Data Security (номер патента – 4405829). Действие патента заканчивается в 2000 году. Правительство США запрещает экспорт алгоритма RSA с ключами более 512 бит.

См. также Криптосистема с открытым ключом, Электронная цифровая подпись, Односторонняя функция с секретом

RC2

Блочный шифр с переменной длиной ключа, разработанный Роном Райвестом. Аббревиатура RC означает «Код Рона» («Ron's Code») или «Шифр Райвеста» («Rivest's Cipher»). Длина блока – 64 бита. Алгоритм является более быстрым, чем алгоритм DES. Стойкость может быть больше или меньше, чем у DES, в зависимости от длины ключа. Алгоритм RC2 является собственностью компании RSA Data Security – для его использования требуется лицензия.

См. также Блочный шифр, DES, RC4, RC5.

RC4

Потоковый шифр, разработанный Роном Райвестом. Длина ключа – переменная. Алгоритм основан на случайных перестановках. Проведенный анализ показывает, что период шифра не менее 10^{100} . Алгоритм RC4 является собственностью компании RSA Data Security – для его использования требуется лицензия.

См. также Потоковый шифр, RC5, RC2.

RC5

Быстрый блочный шифр, разработанный Роном Райвестом. Это алгоритм, зависящий от различных параметров – длины ключа, размера блока и числа циклов шифрования. Длина блока может быть 32, 64 или 128 бит. Число циклов шифрования может изменяться от 0 до 255. Длина ключа от 0 до 2048 бит.

См. также Блочный шифр, RC4, RC2.

Risk analysis

См. Анализ риска

Rainbow series

Серия документов, регулирующих деятельность в области защиты информации в подразделениях Министерства Обороны США.

Recovery plan

См. План обеспечения непрерывной работы и восстановления

Recovery procedures

Действия, предпринимаемые для восстановления способности системы обрабатывать информацию, а также восстановление наборов данных после аварии или сбоя.

См. также План обеспечения непрерывной работы и восстановления.

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.

В Руководящих документах Гостехкомиссии РФ данный термин переводится как «Концепция диспетчера доступа».

См. также Security kernel, Руководящий документ, Государственная техническая комиссия при Президенте РФ.

Reputation

Отказ от факта получения или отправления сообщения.

Rubber hose cryptanalysis

Метод криптоанализа, который заключается в том, что криптоаналитик шантажирует или угрожает владельцу ключа. Это очень мощная атака и, зачастую, самый лучший способ расшифровать шифртекст.

См. также Криптоанализ.

Red

Японская криптографическая роторная машина. Использовалась во время второй мировой войны.

См. также Роторная машина

Running key generator

См. Генератор ключевого потока

Rabin signature scheme

Схема цифровой подписи, предложенная Рабином. Является вариантом схемы цифровой подписи RSA. Отличием является процесс нахождения секретного ключа. Проверка подписи осуществляется быстрее, чем ее выработка (аналогично RSA). В схеме Рабина открытый ключ n вычисляется как произведение двух простых чисел p и q , которые формируют секретный ключ. Подписываемое сообщение должно иметь квадратный корень по модулю n ; иначе сообщение должно быть изменено. Из всех возможных сообщений только четверть имеет квадратный корень по модулю n .

Выработка цифровой подписи осуществляется по формуле:

$$s = m^{1/2} \bmod n, \text{ где } s \text{ – цифровая подпись}$$

Проверка цифровой подписи осуществляется по формуле:

$$m = s^2 \bmod n.$$

См. также Электронная цифровая подпись, RSA.

RSA-129

Инициатива Мартина Гарднера, который в 1977 в Scientific American опубликовал 129-разрядное простое число (426 бит). Был назначен символический приз в \$100 за факторизацию данного числа. В марте 1995 при помощи 1600 компьютеров, объединенных через сеть Internet это число было факторизовано. На это было потрачено 8 месяцев.

См. также Криптоанализ, Brute-force search, RSA.

RDES

Вариант алгоритма DES, который из-за низкой стойкости практически не используется.

См. также DES, Стойкость.

RADIUS

См. Remote Authentication Dial-in User Service

Remote Authentication Dial-in User Service

Протокол удаленной аутентификации, разработанный компанией Livingston Enterprises. Предназначен для дополнительного усиления системы безопасности, располагает различными средствами для контроля доступа и имеет возможности проведения регистрации. Передан в IETF для разработки на его основе всеобъемлющего стандарта для аутентификации коммутируемых соединений.

См. также Terminal Access Control Access System, TACACS+, Extended Terminal Access Control Access System, Аутентификация.

Remanence

Остаток информации в оборудовании или каналах связи после применения процесса очистки памяти.

См. также Object reuse.

RAMP Program Document

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный 1 марта 1995 года. Предназначен для описания Rating Maintenance Phase (RAMP) в Trusted Product Evaluation Program.

См. также Rainbow series, Trusted Computer Security Evaluation Criteria, National Computer Security Center, Trusted Product Evaluation Program.

Red Book

1. См. The Trusted Network Interpretation of Department of Defense Trusted Computer System Evaluation Guidelines
2. См. Trusted Network Environments Guideline – Guidance for Applying the TNI

S

SET

См. Secure Electronic Transaction

Secure Electronic Transaction

Техническая спецификация для защиты транзакций платежных карточных систем, осуществляющих платежи через открытые сети. SET был разработан компаниями Visa и MasterCard, при поддержке таких фирм как IBM, Microsoft, Netscape, SAIC, GTE, Terisa Systems и Verisign. Данная спецификация открыта и свободна для любого использования при разработке SET-совместимого программного обеспечения.

Для симметричного шифрования используется алгоритм DES, а для асимметричного - RSA. Электронная цифровая подпись – алгоритм RSA, хэш-функция – SHA. Сертификаты соответствуют стандарту X.509 v3.

См. также DES, RSA, SHA, X.509.

SSL

См. Secure Sockets Layer

Secure Sockets Layer

Протокол SSL, предложенный компанией Netscape Communications Corp., является независимым от приложений протоколом, который располагается между прикладным (HTTP, FTP, Telnet) и транспортным (TCP, UDP) уровнями модели OSI. Данный протокол обеспечивает шифрование передаваемой информации, аутентификацию абонентов и контроль целостности данных для установленного соединения. Протокол SSL (версия 3.0) предложен на рассмотрение рабочей группы W3C в качестве стандарта Internet.

Для шифрования используются алгоритмы RC2, RC4, IDEA, DES, Triple DES. Шифрование ключей и электронная цифровая подпись – алгоритм RSA, хэш-функция – MD5. Сертификаты соответствуют стандарту X.509.

См. также DES, RSA, X.509, IDEA, MD5, RC2, RC4.

S/WAN

Инициатива, предложенная для реализации архитектуры IPSEC и совместимости различных межсетевых экранов и других средств защиты информации в Internet. S/WAN работает на уровнях ниже тех, на которых работает SSL и S-HTTP, тем самым позволяя использовать их совместно с S/WAN.

См. также IPSEC, SSL, S-HTTP.

Secure Wide Area Network

См. S/WAN

S\MIME

Спецификации для обеспечения безопасности сообщений электронной почты в формате MIME. Данная спецификация разработана компанией RSA Data Security и не является стандартом Internet. В настоящий момент эта спецификация проходит тестирование в IETF на возможность стать стандартом.

Данная спецификация, в случае принятия ее в качестве стандарта Internet, станет конкурентом стандарту MOSS.

См. также MOSS.

Stream cipher

См. Поточковый шифр

SKIPJACK

Алгоритм шифрования, разработанный NSA и реализованный в чипе Clipper. Использует 80-битный ключ для шифрования 64-битных блоков данных. Число циклов шифрования – 32. Является более надежным, чем алгоритм DES.

Достаточно сильно критикуется из-за того, что описание алгоритма не опубликовано и держится в секрете. Считается, что алгоритм может содержать непреднамеренные уязвимости или специально оставленные люки. Другим недостатком данного алгоритма является тот факт, что он может быть реализован только в оборудовании, уполномоченном правительством.

Летом 1995 года в Internet появился алгоритм S1, который многие считают, что это Skipjack.

Является частью проекта Capstone. Опубликован в FIPS PUB 185.

См. также Capstone, Clipper, DES.

S1

См. SKIPJACK

SEAL

1. См. Software-optimized Encryption Algorithm
2. См. Screening External Access Link
3. Криптографическая контрольная сумма, обеспечивающая целостность сообщения, но не защищающая от его подделки.

Software-optimized Encryption Algorithm

Быстрый потоковый шифр, разработанный в 1993 году Рогэвеем (Rogaway) и Копперсмитом (Coppersmith). Разработан специально для использования в 32-разрядных компьютерах.

См. также Поточковый шифр.

Screening External Access Link

Межсетевой экран, разработанный компанией Digital, предназначенный для защиты внутренней сети от проникновения злоумышленников извне и для разграничения доступа внутренних пользователей к серверам Internet.

См. также Экран межсетевой.

SAFER

Блочный шифр, разработанный Массеем в 1993 году, для корпорации Cylink. Размер блока и размер ключа – по 64 бита. Число циклов шифрования – переменное, но не более 10 (рекомендуется не менее 6). В отличие от большинства современных криптосистем в системе SAFER процедуры шифрования и расшифрования немного различаются.

Существуют несколько версий данного алгоритма – SAFER K-64, использующая ключи длиной 64 бита, SAFER K-128, использующая ключи длиной 128 бит. Алгоритм стоек к линейному и дифференциальному анализу (при числе циклов шифрования более 6). В 1995 году была найдена уязвимость в выработке дополнительных ключей. Версии алгоритма с улучшенными методами выработки дополнительных ключей называются SAFER SK-64 и SAFER SK-128, где аббревиатура SK обозначает «усиленные дополнительные ключи» («strengthened key schedule»). Недавно была разработана версия SAFER SK-40, использующая 40-битный ключ и 5 циклов шифрования. Данная версия также устойчива к линейному и дифференциальному криптоанализу.

См. также Блочный шифр, Криптоанализ.

Secure And Fast Encryption Routine

См. SAFER

SHA

Алгоритм разработанный NIST, определенный в стандарте SHS и опубликованный в FIPS PUB 180. В 1994 году был опубликован алгоритм SHA-1, исправивший неопубликованный дефект. Алгоритм SHA очень похож на алгоритмы семейства MD4.

При помощи данного алгоритма можно обрабатывать сообщения длиной до 2^{64} бит. Длина значения хэш-функции – 160 бит. Алгоритм работает медленнее MD5, но более безопасен. Является частью проекта Capstone. Опубликован в FIPS PUB 180.

См. также Хэш-функция, MD4, Capstone, MD5, SHS.

SHS

Американский стандарт на хэш-функции. Является частью проекта Capstone. Опубликован в FIPS PUB 180.

См. также Capstone, SHA.

Secure HyperText Transfer Protocol

Протокол, разработанный компанией Enterprise Integration Technologies, предназначен для защиты гипертекстовой информации. Отличие протокола S-HTTP от SSL заключается в том, что S-HTTP обеспечивает защиту на прикладном уровне протокола HTTP, в то время как SSL работает ниже прикладного уровня и не зависит от используемого протокола обмена

данными. В силу принадлежности к разным уровням модели OSI, данные протоколы могут дополнять друг друга.

См. также SSL.

S-HTTP

См. Secure HyperText Transfer Protocol

Simple Key management for Internet Protocol

Протокол управления ключами, предназначенный для использования в IP-сетях. Был разработан компанией Sun Microsystems в 1994 году. В основе протокола лежит алгоритм Диффи-Хеллмана. Протокол реализуется следующим образом. Абоненты защищенного обмена информацией вырабатывают общий сеансовый ключ по алгоритму Диффи-Хеллмана, который задает условия защищенного обмена, но не используется для шифрования информации. Для шифрования конкретного пакета (или группы пакетов) узел, зашифровывающий информацию, вырабатывает т.н. пакетный ключ K_p , которым шифруют данные, помещаемые в блок данных SKIP-пакета. Сам же пакетный ключ K_p шифруется с помощью сеансового ключа и также записывается в пакет, снабжаемый SKIP-заголовком. Заголовок SKIP-пакета идентичен заголовку IP-пакета, однако добавляет несколько дополнительных полей, содержащих информацию об используемых алгоритмах шифрования и режиме работы протокола SKIP.

В спецификации протокола SKIP описаны 3 режима работы: с инкапсуляцией, с аутентификацией и с шифрованием и аутентификацией. Также оговаривается, но не описан режим сжатия данных. Режим инкапсуляции (туннелирования) предназначен для создания VPN. Режим аутентификации предназначен для контроля целостности незашифрованных данных при помощи MAC.

См. также Диффи-Хеллмана алгоритм, Открытое распределение ключей, Virtual Private Network, MAC, Управление ключами, Oakley.

SKIP

См. Simple Key management for Internet Protocol

Sniffing

Прослушивание трафика с целью сбора передаваемых паролей, ключей и другой идентификационной или аутентификационной информации.

Анализ трафика может осуществляться одним из двух способов: путем “замыкания” на себя, (т.е. на узел злоумышленника) трафика части сети, где каждый узел в принципе может “прослушивать” кадры данных, адресованные другим узлам, либо путем получения непосредственного доступа к тем областям памяти узла или маршрутизатора, через которые проходят IP-пакеты, и осуществить расшифровку трафика - по телу IP-пакетов восстановить последовательность действий обоих абонентов соединения. Для подобного рода атак разработаны специальные средства, получившие название sniffer, которые можно найти без особого труда в сети Internet.

Данная угроза основывается на том, что в большинстве случаев идентификатор и пароль пользователя передается по сети в открытом виде. Даже если программное обеспечение позволяет шифровать эти данные, то при его инсталляции администраторы сети

забывают установить необходимые параметры (например, в сетевой ОС Novell NetWare 3.12 по умолчанию установлена опция «Не шифровать пароль пользователя»).

Spoofting

Подмена адреса отправителя как правило реализуется 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. Данный способ атаки чрезвычайно опасен как в силу возможности нанесения значительного ущерба (злоумышленник становится “своим”), так и значительных сложностей при организации противодействия.

См. также IP-spoofing.

Salami attack

Атака, используемая в финансовой сфере. Принцип атаки заключается в неправильном округлении дробных сумм при исчислении процентов на счета. Результат атаки зависит от числа обрабатываемых счетов.

Security policy

В Руководящих документах Гостехкомиссии данный термин переводится «Правила разграничения доступа».

См. Политика безопасности

Security clearance

См. Уровень прозрачности

Subject

См. Субъект

Secure state

См. **Ошибка! Источник ссылки не найден.**

Security flaw

Ошибка при назначении полномочий или упущение при разработке, реализации или управлении средствами защиты системы, которые могут привести к преодолению защиты.

Security hole

См. Security flaw

Security kernel

Программные и аппаратные элементы ДВБ (ТСВ), реализующие концепцию монитора ссылок. Они должны разделять все попытки доступа субъектов к объектам, быть защищенным от модификации и проверены на корректное выполнение своих функций.

В Руководящих документах Гостехкомиссии данный термин переводится как «диспетчер доступа».

См. также Достоверная вычислительная база.

Security level

См. Уровень безопасности

Secret-key cryptography

См. Криптосистема с секретным ключом

Symmetric cryptography

См. Криптосистема с секретным ключом

Sigaba

Американская криптографическая роторная машина. Использовалась во время второй мировой войны.

См. также Роторная машина

Subtilitas de subtilitae rerum

Книга по криптологии, написанная в 1554 году итальянским математиком Джироламо Кардано.

См. также Polygraphia, Opus novum.

Synchronous stream cipher

См. Синхронизирующаяся потоковая криптосистема

Self synchronous stream cipher

См. Самосинхронизирующаяся потоковая криптосистема

Self enforcing protocol

См. Протокол, самообеспечивающий законность

Self-authenticating signature scheme

Цифровая подпись, подлинность которой может быть проверена в любое время без согласия подписывающего лица. Любая цифровая подпись с открытым ключом может быть отнесена к этой категории.

См. также Электронная цифровая подпись, Криптосистема с открытым ключом.

s^n DES

Вариант алгоритма DES, предложенный группой корейских исследователей. Разработан таким образом, что одинаково хорошо противостоит атакам при помощи дифференциального и линейного криптоанализа.

См. также Криптоанализ, DES.

Secret Sharing Scheme

В процессе поиска надежного и безопасного механизма управления ключами в 1979 году независимо двумя математиками Блэкли (Blakley) и Шамиром (Shamir) была предложена схема разделения секрета. Основная идея данной схемы – разделить секретный ключ между несколькими субъектами, чтобы собравшись вместе они могли восстановить ключ из нескольких частей.

См. также Управление ключами, Shamir's Secret Sharing Scheme.

Shamir's Secret Sharing Scheme

Схема с разделением секрета, предложенная Шамиром и основанная на полиномиальной интерполяции.

См. также Secret Sharing Scheme.

Secure Courier

Протокол, предложенный Netscape для ведения электронной торговли через Internet. Аналогично протоколу iKP базируется на криптографии с открытым ключом.

См. также iKP.

Security zone

См. Зона безопасности

Stateful Inspection firewall

Один из вариантов реализации межсетевого экрана. Исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Проверяет содержимое пропускаемых через себя пакетов на трех уровнях модели OSI – сетевом, сеансовом и прикладном. Использует специальные алгоритмы фильтрации пакетов.

См. также Экран межсетевой.

Security Coordination Center

SCC (Security Coordination Center) был создан в 1989 году Агентством коммуникаций Министерства Обороны США для координации и централизованного управления группами реагирования на инциденты. Однако своей цели не достиг и в настоящий момент является обычным центром по обеспечению информационной безопасности подразделений Министерства Обороны США.

SCC

См. Security Coordination Center

Silver Book

См. Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX[®] System

T

Triple DES

Вариант алгоритма DES, в котором открытый текст подвергается процессу шифрования три раза. Известно несколько режимов использования данного алгоритма: DES-EEE3, DES-EDE3, DES-EEE2, DES-EDE2. В этих режимах могут использовать три или два разных ключа.

Атаки на двухключевые режимы были предложены Мерклем и Хеллманом в 1981 году и Ван Ооршотом (Van Oorschot) и Винером (Wiener) в 1991 году.

См. также DES, DES-EEE3, DES-EDE3, DES-EEE2, DES-EDE2.

Trapdoor

См. Люк

Trojan horse

См. Троянский конь

Trusted Computing Base

См. Достоверная вычислительная база

TCB

См. Достоверная вычислительная база

TEMPEST

Стандарт США для защиты компьютеров от побочных электронных сигналов, излучаемых электрическим и электронным оборудованием.

Threat

См. Угроза АС

Trusted path

Механизм, с помощью которого пользователь за терминалом может взаимодействовать непосредственно с ДВБ (TCB). Он может быть активизирован только пользователем или ДВБ, его работа не может быть прервана, имитирована или нарушена недостоверным программным обеспечением.

См. также Достоверная вычислительная база.

Trusted Computer Security Evaluation Criteria

Документ, разработанный Центром Компьютерной Безопасности Министерства Обороны США (DoD Computer Security Center) в соответствии с директивой 5215.1 и утвержденный 15 августа 1983 года. Отчет (также называемый Оранжевой книгой из-за цвета своей обложки), является руководством по безопасности, предназначенным как для покупателей, так и для разработчиков. В данном документе описываются критерии, в соответствии с которыми оцениваются операционные системы и аппаратно-программные средства, изменяющие функции операционных систем. Оценка безопасности СУБД и вычислительных сетей производится по другим документам.

В документе изложены единые для Министерства Обороны США требования к обеспечению безопасности компьютерных систем и порядок определения классов защищенности компьютерных систем МО США.

В документе выделены общие требования по обеспечению безопасности обрабатываемой информации, определен перечень показателей защищенности, характеризующих реализацию этих требований. Совокупность показателей определяет класс безопасности рассматриваемой системы. Выделяются семь классов с различными механизмами обеспечения информационной безопасности. Самый нижний класс D присваивается системам, которые не соответствуют ни одному уровню безопасности. Остальные шесть классов образуют 4 группы:

- Класс А. Означает гарантированную защиту. Данный класс предназначен для систем, к которым предъявляются достаточно высокие требования по безопасности.
- Класс В. Характеризуется полномочным управлением доступом. Делится на три подкласса В1, В2 и В3 (от более низкого к более высокому подклассу).
- Класс С. Характеризуется избирательным управлением доступом. Применяется к оценке большинства коммерческих систем. Делится на два подкласса С1 и С2.

Класс безопасности присваивается системе при прохождении ею процесса сертификации в NCSC.

Подход, описанный в TCSEC страдает рядом недостатков:

- Данный документ не применим к персональным компьютерам;
- Игнорирование проблемы целостности информации. Упор делается на конфиденциальность информации.
- Основной акцент делается на «безопасность при приобретении», а не на «безопасность при эксплуатации».

В целом TCSEC ориентирован на применение в военных организациях и не учитывает специфики коммерческих организаций.

TCSEC

См. Trusted Computer Security Evaluation Criteria

The Trusted Network Interpretation of Department of Defense Trusted Computer System Evaluation Guidelines

Издание National Computer Security Center, интерпретирующее TCSEC для вычислительных сетей. Также известно как Красная книга. Состоит из двух отдельных книг в красной обложке, которые вышли под названиями Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria (NCSC-TG-005), утвержденный 31 июля 1987

года, и Trusted Network Interpretation Environments Guideline: Guidance for Applying the Trusted Network Interpretation (NCSC-TG-011) утвержденный 1 августа 1990 года,.

Красная книга была выпущена в качестве руководства для оценки компьютерных сетей Министерства Обороны США.

Timestamping

Механизм, использующий метки времени для контроля актуальности информации. Метки содержат дату и время создания (или отправления) информации. Отличительными особенностями данного механизма являются отсутствие взаимосвязи с какой-либо секретной информацией и возможность неопределенного продления срока действия отмеченного документа.

Timed-release cryptosystem

См. Криптосистема с временным раскрытием

Timelock puzzles

См. Шарады с временным замком

Technical Criteria for Evaluation of Commercial Security Products

«Технические критерии для оценки коммерческих изделий обеспечения безопасности информации» разработаны Commercial Computer Security Centre. Основные положения данного документа соответствуют Orange Book.

См. также Commercial Computer Security Centre, Trusted Computer Security Evaluation Criteria.

Trap door one-way function

См. Односторонняя функция с секретом

Tessera

См. Fortezza

Terminal Access Control Access System

Протокол удаленной аутентификации, разработанный Internet-провайдером – фирмой BBN Planet и использованный фирмой Cisco Systems. В настоящий момент – это единственный протокол, принятый IETF в качестве стандарта. Описан в RFC 927 и RFC 1492. Позволяет проверять имя и пароль удаленного пользователя.

См. также TACACS+, Extended Terminal Access Control Access System, RADIUS, Аутентификация.

TACACS

См. Terminal Access Control Access System

TACACS+

Протокол удаленной аутентификации, разработанный компанией Cisco Systems для поддержания дополнительных мер безопасности, в частности таких, как защита сетевых коммуникаций (предотвращение перехвата паролей), улучшение контроля доступа и ведения регистрации. Поддерживается только компанией Cisco Systems.

См. также Terminal Access Control Access System, Extended Terminal Access Control Access System, RADIUS, Аутентификация.

Transport Layer Secure Protocol

Протокол, объединяющий в себе возможности протоколов SSL компании Netscape и PCT компании Microsoft. В настоящий момент рассматривается в IETF.

См. также Secure Sockets Layer, Private Communication Technology.

TLSP

См. Transport Layer Secure Protocol

Traffic analysis

См. Анализ трафика

Technical Rational Behind CSC-STD-003-85: Computer Security Requirements – Guidance for Applying the DoD TCSEC in Specific Environments

Документ, разработанный Центром Компьютерной Безопасности Министерства Обороны США (DoD Computer Security Center) в соответствии с директивой 5215.1 и утвержденный 25 июня 1985 года. Это руководство определяет минимальные требования безопасности к компьютерам Министерства Обороны США на которых обрабатывается секретная информация.

См. также Rainbow series, Trusted Computer Security Evaluation Criteria, Computer Security Requirements – Guidance for Applying the DoD TCSEC in Specific Environments.

Trusted Product Evaluations – A Guide for Vendors

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный 22 июня 1990 года. Этот документ описывает процедуры связи с NCSC по поводу оценки информационных систем по программе Trusted Product Evaluation Program.

См. также Rainbow series, National Computer Security Center, Trusted Product Evaluation Program.

Trusted Product Evaluation Program

Программа оценки коммерческих информационных систем в соответствии с TCSEC.
См. также Technical Criteria for Evaluation of Commercial Security Products, Trusted Computer Security Evaluation Criteria, Preferred Products List, Evaluated Products List.

TPEP

См. Trusted Product Evaluation Program

TNI

См. The Trusted Network Interpretation of Department of Defense Trusted Computer System Evaluation Guidelines

Trusted Network Environments Guideline – Guidance for Applying the TNI

См. The Trusted Network Interpretation of Department of Defense Trusted Computer System Evaluation Guidelines

Trusted Product Evaluation Questionnaire

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и вторая версия которого утверждена 2 мая 1992 года. Этот документ описывает вопросы, которыми должен руководствоваться покупатель при выборе системы защиты информации.

См. также Rainbow series, National Computer Security Center, Trusted Product Evaluation Program.

Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX® System

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный 19 августа 1989 года. Первый документ, выпущенный TRUSIX и определяющий механизмы реализации списков контроля доступа в операционной системе UNIX.

См. также Rainbow series, National Computer Security Center, Access control list.

Trusted Database Management System Interpretation of the TCSEC

Документ, разработанный Национальным центром компьютерной безопасности в соответствии с директивой 5215.1 и утвержденный в апреле 1991 года. Издание National Computer Security Center, интерпретирующее TCSEC для использования в системах управления базами данных.

См. также Rainbow series, Trusted Computer Security Evaluation Criteria, National Computer Security Center.

TDI

См. Trusted Database Management System Interpretation of the TCSEC

Tan Book

См. A Guide to Understanding Audit in Trusted Systems

Teal Green Book

См. Glossary of Computer Security Terms

Turquoise Book

См. A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems

U

Unauthorized access

См. Несанкционированный доступ

Undeniable Signature Scheme

См. Бесспорная подпись

V

Verification

См. Верификация

Vulnerability

См. Уязвимость АС

Violator

См. Нарушитель

Virtual Private Network

Механизм защищенного обмена (по туннелю) трафиком между локальными сетями по сетям общего пользования (Internet). Для создания VPN существует 4 различных протокола: PPTP, L2F, L2TP и IPSec.

См. также IP Security Protocol, Layer 2 Forwarding, Layer 2 Tunneling Protocol, Point-to-Point Tunneling Protocol.

VPN

См. Virtual Private Network

Venice Blue Book

См. Computer Security Subsystem Interpretation of the TCSEC

Violet Book

См. Accessing Controlled Access Protection

W

- См. Червь
- Worm**
- См. Information Technology Security Evaluation Criteria
- White Book**
- Whitening**

X

X.400

Рекомендация ИТУ-Т X.400 Message Handling System (MHS) определяют один из двух международных стандартов хранения и отправки электронной почты (второй стандарт - SMTP). Он обеспечивает поддержку различных способов защиты для ее представления, передачи и доставки. Стандарт X.400 иногда называют Красной книгой (из-за цвета обложки документа).

X.435

Рекомендация ИТУ-Т, базирующаяся на рекомендации X.400 и предназначена для защиты электронного обмена данными (electronic data interchange, EDI).

X.509

Рекомендация ИТУ-Т описывает механизм аутентификации для службы каталогов X.500. Также широко известна как документ, описывающий формат сертификатов. Первая версия была опубликована в 1988 году. Текущая, третья, версия – в 1995 году. Процесс аутентификации может базироваться как на криптосистемах с секретным ключом, так и на криптосистемах с открытым ключом. В последнем случае, аутентификация основана на механизме сертификатов.

Стандарт X.509 поддерживается многими протоколами, включая PEM, PKCS, S-HTTP и SSL.

См. также Аутентификация, Сертификат, PKCS, PEM, SSL, S-HTTP.

Extended Terminal Access Control Access System

Расширенный протокол аутентификации TACACS. Позволяет разграничивать доступ для авторизованных пользователей и ряд дополнительных функций на стороне сервера.

См. также TACACS, TACACS+, RADIUS.

XTACACS

См. Extended Terminal Access Control Access System

X-Force

В 1994 году один из организаторов CERT/CC – Кристофер Клаус основал компанию Internet Security Systems, Inc., которая является одним из лидеров в области разработки средств анализа защищенности и обнаружения атак. В компании ISS существует научно-исследовательская группа X-Force, объединяющая экспертов в области обеспечения информационной безопасности. Эта группа не только постоянно отслеживает все публикуемые другими группами сообщения об обнаруженных уязвимостях, но и сама проводит тестирование программных и аппаратных средств. Результаты этих

исследований помещаются в базу данных уязвимостей и угроз (ISS X-Force Threat and Vulnerability Database).

См. также CERT, CIAC.

Y

Yellow Book

1. См. Technical Rational Behind CSC-STD-003-85: Computer Security Requirements – Guidance for Applying the DoD TCSEC in Specific Environments
2. См. A Guide to Understanding Trusted Recovery in Trusted Systems

Yellow-Green Book

См. Guidelines for Writing Trusted Facility Manuals

5

5200.28-STD

См. Orange book

Список литературы

1. В.Ю. Гайкович, А. Першин. Безопасность электронных банковских систем. М.: Единая Европа, 1994
2. А.А. Варфоломеев, М.Б. Пеленицын. Методы криптографии и их применение в банковских технологиях. М.: МИФИ, 1995
3. Д.Б. Халяпин, В.И. Ярочкин. Основы защиты промышленной и коммерческой информации. Термины и определения. М.: ИПКПР, 1994
4. С.В. Лекарев, В.А. Порк. Бизнес и безопасность. Толковый терминологический словарь. М.: ЦКСИиМ. Ягуар, 1995
5. А.А. Саломаа. Криптография с открытым ключом. М.: Мир, 1996
6. В. Schneier. Applied cryptography. John Wiley & Sons, Inc. 1996
7. Answers to Frequently Asked Questions About Today's Cryptography. Version 3.0. RSA Laboratories. 1995
8. Толковый словарь по вычислительным системам. М.: Машиностроение, 1990
9. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Гостехкомиссия РФ.
10. В.И. Ярочкин, Т.А. Шевцова. Словарь терминов и определений по безопасности и защите информации.
11. И.Л. Аснис, С.В. Федоренко, К.Б. Шабунюв. Краткий обзор криптосистем с открытым ключом. Защита информации. Конфидент, №2, 1994
12. Брандмауэры, или запирайте вашу дверь. Обзор. Сети, №2, 1997
13. Дэн Бэкман. Обеспечение безопасности посредством удаленной аутентификации. Сети и системы связи, №5, 1997
14. Арт Уитман. Протокол PPP и безопасность. Сети и системы связи, №8, 1996
15. А. Чмора. Криптосистема с депонированием ключа. CONNECT, №3, 1997
16. А. Чмора. Безопасная электронная почта. CONNECT, №8, 1996
17. А. Чмора. Безопасная электронная почта. CONNECT, №9, 1996
18. Consolidated Security Glossary. IEEE POSIX P1003.6 Security Working Group
19. Положение о государственном лицензировании деятельности в области защиты информации.
20. В.И. Парфенов. Защита информации. Термины и определения. Словарь. Вопросы защиты информации, №3,4, 1996, №3-4, 1997.
21. "Безопасность информации-97". Материалы конференции.
22. Б. Киви. Еще один шаг к новому криптостандарту AES. ComputerWeekly, №40, 1998.

Указатель

5

5200.28-STD, 168

A

A Guide to Procurement of Trusted Systems
An Introduction to Procurement Initiators on Computer Security Requirements, 90
Computer Security Contract Data Requirements List and Data Item Description Tutorial, 90
How to Evaluate a Bidder's Proposal Document – An Aid to Procurement Initiators and Contractors, 90
Language for RFP Specifications and Statements of Work – An Aid to Procurement Initiators, 90
A Guide to Understanding Audit in Trusted Systems, 87
A Guide to Understanding Configuration Management in Trusted Systems, 88
A Guide to Understanding Covert Channel Analysis of Trusted Systems, 92
A Guide to Understanding Data Remanence in Automated Information Systems, 91
A Guide to Understanding Design Documentation in Trusted Systems, 88
A Guide to Understanding Discretionary Access Control in Trusted Systems, 88
A Guide to Understanding Identification and Authentication in Trusted Systems, 89
A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems, 91
A Guide to Understanding Object Reuse in Trusted Systems, 89
A Guide to Understanding Security Modeling in Trusted Systems, 89
A Guide to Understanding Security testing and Test Documentation in Trusted Systems, 90
A Guide to Understanding Trusted Distribution in Trusted Systems, 88
A Guide to Understanding Trusted Facility Manuals, 89
A Guide to Understanding Trusted Recovery in Trusted Systems, 89
A Guide to Writing the Security Features User's Guide for Trusted Systems, 91
Access control, 86
Access control list, 86
Access period, 86
Accessing Controlled Access Protection, 91
Accountability, 86
Adaptive chosen ciphertext attack, 87
Adjudicated protocol, 87
Advanced Encryption Standard, 92
AES, 92
Amber Book, 92
American National Standards Institute, 84
ANSI, 84
ANSI X12.58, 85
ANSI X9.17, 84
ANSI X9.23, 84

ANSI X9.30, 84
ANSI X9.31, 84
ANSI X9.41, 85
ANSI X9.42, 85
ANSI X9.44, 85
ANSI X9.45, 85
ANSI X9.9, 84
Application-level Gateway, 87
Aqua Book, 92
Arbitrated protocol, 87
AS2805.6.5.3, 87
ASSIST, 85
Assurance, 87
Asymmetric cryptography, 87
Audit, 86
Audit trail, 86
Authentication, 86
Authentication Header, 119
Authenticode, 85
Authorization, 87
Automated Systems Security Incident Support Team, 86

B

Backup plan, 93
Banking Circular 226, 93
Banking Circular 229, 93
Bastion Host, 95
BC-226, 93
BC-229, 93
Bell-LaPadulla model, 93
Birthday attack, 94
Blind signature scheme, 94
Block Cipher, 93
Blowfish, 93
Blue Book, 95
Bright Blue Book, 95
Bright Orange Book, 95
Brown Book, 95
Brute-force attack, 94
Brute-force search, 94
Burgundy Book, 95

C

C-36, 101
Capability, 99
CAPI, 101
Capstone, 97
CBC, 96
CERT, 97
Certificate, 101
Certificate Revocation List, 101
CFB, 96
Challenge-Handshake Authentication Protocol, 102
CHAP, 102
Chosen ciphertext attack, 100
Chosen key attack, 101
Chosen message attack, 100
Chosen plaintext attack, 100

CIAC, 98
Cipher, 96
Cipher Block Chaining, 96
Cipher Feedback, 96
Ciphertext, 96
Ciphertext auto key, 101
Ciphertext only attack, 101
Circuit-level Gateway, 102
Clipper, 97
COAST, 103
Code signing, 97
Commercial Computer Security Centre, 99
Commercial Product Evaluation, 99
Compromise, 99
Computer Emergency Response Team, 97
Computer Fraud and Abuse Act of 1986, 100
Computer Incident Advisory Capability, 98
Computer Misuse Act of 1990, 100
Computer Operations Audit and Security Technology, 102
Computer Security Act of 1987, PL 100-235, 100
Computer Security Agency, 99
Computer Security Requirements – Guidance for Applying the DoD TCSEC in Specific Environments, 103
Computer Security Subsystem Interpretation of the TCSEC, 103
Confidentiality, 99
Contingency plan, 99
Counter method, 101
Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, 100
Covert channels, 98
Covert storage channel, 98
Covert timing channel, 99
Cryptographic application programming interface, 102
Cryptography, 98
Cryptoki, 102
CSC-STD-001-83, 103
CSC-STD-002-85, 103
CSC-STD-003-85, 103
CSC-STD-004-85, 103
CTAK, 101

D

DAC, 106
Dark Lavender Book, 108
Data Computer Act of 1984, 106
Data Encryption Standard, 104, 105
Data security officer, 106
Davies-Meyer hash function, 107
Demilitarized zone, 107
Denial of service, 105
Department of Defense, 105
DES, 104
DES-EDE2, 107
DES-EDE3, 107
DES-EEE2, 107
DES-EEE3, 106
Designated Confirmer Signature, 106
DESX, 105
Differential cryptanalysis, 106
Diffie-Hellman, 104
Digital envelop, 108
Digital fingerprint, 107
Digital Signature Algorithm, 104
Digital Signature Standard, 104
Discretionary access control, 105

Disk scavenging, 105
DMZ, 108
DoD, 105
DoD Guidelines for Computer Security, 105
Domain, 106
DSA, 104
DSO, 106
DSS, 104
Dual-homed Gateway, 107

E

E31.20, 110
ECB, 109
EES, 110
Electronic codebook, 109
Electronic Communications Privacy Act of 1986, 110
ElGamal, 109
Elliptic Curves, 109
Enigma, 110
EPL, 109
Escrowed Encryption Standard, 110
ETEBAC 5, 110
Evaluated Products List, 109
Exhaustive key search, 110
Exponential key agreement, 110
Extended Terminal Access Control Access System, 165

F

Fail-stop signature scheme, 112
FAPKC, 111
Fast Data Encipherment Algorithm, 111
Fault, 111
FEAL, 111
FedCIRC, 113
Federal Computer Incident Response Capability, 112
Firewall, 112
FIRST, 112
Flaw, 111
Foreign Corrupt Practices Act of 1977, 111
Forest Green Book, 113
Fortezza, 111
Forum of Incident Response and Security Teams, 112

G

Garbage collecting, 114
G-DES, 114
Glossary of Computer Security Terms, 115
Greedy program, 114
Green Book, 114
Group signature, 114
Guessed plaintext attack, 114
Guidelines for Formal Verification Systems, 115
Guidelines for Writing Trusted Facility Manuals, 115

H

Hash, 116
Hole, 116
Hot Peach Book, 116

I

IDEA, 117
Identification, 118
IEEE 802.10c, 117
IEEE P1363, 117
IKE, 120
iKP, 117
Information Technology Security Evaluation Criteria, 118
Integrity, 120
Internal feedback, 118
International Data Encryption Algorithm, 117
International Organization for Standardization, 117
Internet Key Exchange, 120
Internet Keyed Payments Protocol, 117
Internet Security Association & Key Management Protocol, 119, 120
Introduction to Certification and Accreditation Concepts, 120
Intrusion, 119
Intrusion Detection, 119
Intrusion Detection System, 119
IP Security Protocol, 119
IPSEC, 119
IP-spoofing, 118
ISAKMP, 120
ISO, 117
Iterated Block Cipher, 118
ITSEC, 118

K

KAK, 121
Kerberos, 121
Key, 121
Key auto key, 121
Key crunching, 122
Key deletion, 122
Key distribution, 122
Key escrow, 122
Key generation, 122
Key management, 122
Key recovery, 122
Key schedule, 121
Key storage, 122
Key stream generator, 121
Knapsack, 121
Known plaintext attack, 121

L

L2F, 125
L2TP, 125
Label, 124
Layer 2 Forwarding, 124
Layer 2 Tunneling Protocol, 125
Least privilege, 124
LFSR, 124
Light Blue Book, 125
Light Pink Book, 125
Light Yellow Book, 125
Linear Feedback Shift Register, 124
Link encryption, 124
Loophole, 124
LUC, 124

M

M-209 Converter, 127
MAC, 126
Mandatory access control, 127
Man-in-the-middle, 128
Masquerade, 127
McEliece cryptosystem, 126
MD2, 126
MD4, 127
MD5, 127
Merkle Tree, 126
Message Authentication Code, 127
Message Digest, 128
Message integrity check, 128
Message Security Protocol, 128
Middleperson attack, 128
MIME Object Security Service, 126
MOSS, 126
MSP, 128
Multilevel security, 127

N

NASA Automated Systems Incident Response Capability, 129
NASIRC, 129
National Computer Security Center, 130
National Institute of Standards and Technology, 129
National Security Agency, 129
NBS, 129
NCSC, 130
NCSC-TG-001, 130
NCSC-TG-002, 130
NCSC-TG-003, 130
NCSC-TG-004, 131
NCSC-TG-005, 131
NCSC-TG-006, 131
NCSC-TG-007, 131
NCSC-TG-008, 131
NCSC-TG-009, 131
NCSC-TG-010, 131
NCSC-TG-011, 131
NCSC-TG-013, 131
NCSC-TG-014, 131
NCSC-TG-015, 131
NCSC-TG-016, 131
NCSC-TG-017, 132
NCSC-TG-018, 132
NCSC-TG-019, 132
NCSC-TG-020, 132
NCSC-TG-021, 132
NCSC-TG-022, 132
NCSC-TG-023, 132
NCSC-TG-024, 132
NCSC-TG-025, 132
NCSC-TG-026, 132
NCSC-TG-027, 133
NCSC-TG-028, 133
NCSC-TG-029, 133
NCSC-TG-030, 133
Neon Orange Book, 133
network address translation, 141
New Directions in Cryptography, 130
Niederreiter cryptosystem, 130
NIST, 129

Nonrepudiation, 130
NSA, 129

O

Oakley, 135
Object, 134
Object reuse, 134
Object Signing, 134
OFB, 134
OMBA-123, 135
One-time pad, 134
One-time signature, 135
One-way function, 135
Opus novum, 135
Orange book, 134
Output Feedback, 134

P

Packet-filtering firewall, 140
PAP, 141
Partial Key Escrow, 141
Password Authentication Protocol, 141
Password Management Guideline, 141
PBC, 140
PCBC, 140
PCT, 138
PEM, 138
PEM-MIME, 138
Personal Information Exchange, 141
PFX, 141
Pink Book, 141
PKCS, 136
PKCS #1, 136
PKCS #10, 137
PKCS #11, 137
PKCS #3, 136
PKCS #5, 136
PKCS #6, 136
PKCS #7, 136
PKCS #8, 136
PKCS #9, 136
Plaintext, 139
Plaintext Block Chaining, 140
Point-to-Point Tunneling Protocol, 138
Polygraphia, 139
PPL, 139
PPTP, 138
Preferred Products List, 138
Principal, 138
Privacy Act of 1974, 139
Privacy Enhanced Mail, 137
Private Communication Technology, 138
Private key, 137
Process, 139
Propagating Cipher Block Chaining, 140
Protocol, 139
Proxy, 140
Proxy Server, 141
Public key, 137
Public-key cryptography, 139
Public-Key Cryptography Standards, 137
Purchase key attack, 139
Purple, 139
Purple Book, 142

Q

Quantum cryptography, 143

R

Rabin signature scheme, 146
RADIUS, 147
Rainbow series, 145
RAMP Program Document, 147
RC2, 144
RC4, 145
RC5, 145
RDES, 146
Recovery plan, 145
Recovery procedures, 145
Red, 146
Red Book, 147
Reference monitor concept, 145
Remanence, 147
Remote Authentication Dial-in User Service, 147
Reputation, 145
Risk analysis, 145
round function, 118
RSA, 144
RSA-129, 146
Rubber hose cryptanalysis, 146
Running key generator, 146

S

S/WAN, 148
S1, 149
SAFER, 150
Salami attack, 152
SCC, 155
Screening External Access Link, 150
SEAL, 149
Secret Sharing Scheme, 154
Secret-key cryptography, 153
Secure And Fast Encryption Routine, 150
Secure Courier, 154
Secure Electronic Transaction, 148
Secure HyperText Transfer Protocol, 150
Secure Sockets Layer, 148
Secure state, 152
Secure Wide Area Network, 148
Security clearance, 152
Security Coordination Center, 155
Security flaw, 152
Security hole, 152
Security kernel, 153
Security level, 153
Security policy, 152
Security zone, 154
Self enforcing protocol, 153
Self synchronous stream cipher, 153
Self-authenticating signature scheme, 154
SET, 148
SHA, 150
Shamir's Secret Sharing Scheme, 154
SHS, 150
S-HTTP, 151
Sigaba, 153
Silver Book, 155

Simple Key management for Internet Protocol, 151
SKIP, 151
SKIPJACK, 149
SMIME, 149
sⁿDES, 154
Sniffing, 151
Software-optimized Encryption Algorithm, 149
Spoofing, 152
SSL, 148
Stateful Inspection firewall, 154
Stream cipher, 149
strengthened key schedule, 150
Subject, 152
Subtilitas de subtilitate rerum, 153
Symmetric cryptography, 153
Synchronous stream cipher, 153

T

TACACS, 159
TACACS+, 159
Tan Book, 161
TCB, 156
TCSEC, 157
TDI, 161
Teal Green Book, 161
Technical Criteria for Evaluation of Commercial Security Products, 158
Technical Rational Behind CSC-STD-003-85: Computer Security Requirements – Guidance for Applying the DoD TCSEC in Specific Environments, 159
TEMPEST, 156
Terminal Access Control Access System, 158
Tessera, 158
The Trusted Network Interpretation of Department of Defense Trusted Computer System Evaluation Guidelines, 157
Threat, 156
Timed-release cryptosystem, 158
Timelock puzzles, 158
Timestamping, 158
TLSP, 159
TNI, 160
TPEP, 160
Traffic analysis, 159
Transport Layer Secure Protocol, 159
Trap door one-way function, 158
Trapdoor, 156
Triple DES, 156
Trojan horse, 156
Trusted Computer Security Evaluation Criteria, 157
Trusted Computing Base, 156
Trusted Database Management System Interpretation of the TCSEC, 160
Trusted Network Environments Guideline – Guidance for Applying the TNI, 160
Trusted path, 156
Trusted Product Evaluation Program, 160
Trusted Product Evaluation Questionnaire, 160
Trusted Product Evaluations – A Guide for Vendors, 159
Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX[®] System, 160
Turquoise Book, 161

U

Unauthorized access, 162
Undeniable Signature Scheme, 162

V

Venice Blue Book, 163
Verification, 163
Violator, 163
Violet Book, 163
Virtual Private Network, 163
VPN, 163
Vulnerability, 163

W

White Book, 164
Whitening, 164
Worm, 164

X

X.400, 165
X.435, 165
X.509, 165
X-Force, 165
XTACACS, 165

Y

Yellow Book, 167
Yellow-Green Book, 167

A

Абонентское шифрование, 26
Автоматизированная система обработки информации, 25
Авторизация, 23
Авторизованный субъект доступа, 24
Агентство национальной безопасности, 26
Административные меры защиты информации, 26
Администратор безопасности, 25
Аккредитация, 26
Анализ защищенности, 24
Анализ риска, 24
Анализ трафика, 26
Антивирусная программа, 25
Аппаратное средство защиты, 25
Аппаратно-программные меры защиты информации, 26
Атака, 23
Атрибут доступа, 25
Аттестация, 24
Аттестация испытательных лабораторий, 24
Аттестация объекта в защищенном исполнении, 24
Аудит, 25
Аутентификация, 23
Аутентификация взаимная, 23
Аутентификация односторонняя, 23
Аутентификация сильная, 23
Аутентификация слабая, 23

Б

Бастион, 29
Безопасность АС, 27
Безопасность информации, 27
Безопасность информационной технологии, 27
Безопасность ресурса АС, 27
Безопасность субъектов информационных отношений, 27
Белла-Лападулла модель, 28
Беспорная подпись, 29
Блочный шифр, 28
Бомба временная, 28
Бомба логическая, 28
Брандмауэр, 27
Бьюфорта квадрат, 29

В

Верификатор байт-кода, 30
Верификация, 30
Вероятностное шифрование, 30
Вижинера квадрат, 30
Вирус, 30
Владелец информации, 31
Восстановительные процедуры, 30

Г

Гамма шифра, 33
Гаммирование, 34
Гарантии, 34
Генератор ключевого потока, 34
Генерация ключей, 34
ГОСТ 28147-89, 32
ГОСТ Р 34.10-94, 32
ГОСТ Р 34.11-94, 33
ГОСТ Р 50739-95, 33
ГОСТ Р 50922-96, 33
Гостехкомиссия РФ, 27
Государственная техническая комиссия при Президенте РФ, 32
Гриф, 33
Групповая подпись, 34
ГТК РФ, 32

Д

ДВБ, 36
Декодирование, 37
Депонирование ключей, 37
Дерево Меркля, 37
Джефферсона колесо, 36
Дискреционный доступ, 35
Дифференциальный криптоанализ, 37
Диффи-Хеллмана алгоритм, 35
Документированная информация, 37
Домен, 36
Доска Полибия, 37
Достоверная вычислительная база, 36
Достоверность информации, 35
Достоверный маршрут, 36
Доступ, 35
Доступ к ресурсу, 35
Доступность системы, 35

З

Зашифрование, 38
Защита информации, 38
Защищенность, 38
Злоумышленник, 38
Зона безопасности, 38

И

Идентификатор, 39
Идентификация, 39
Избирательный доступ, 39
Имитовставка, 40
Имитозащита, 39
Инструктивные указания Государственного Арбитража СССР № И-1-4, 40
Информация, 39

К

Казиски метод, 44
Канальное шифрование, 43
Кардано решетка, 44
Квадрат Вижинера, 44
Квадрат Полибия, 44
Квантовая криптография, 45
Класс защищенности, 42
Ключ криптографический, 41
Ключевая система, 43
Код, 41
Код аутентификации сообщения, 46
Код целостности сообщений, 46
Кодирование, 41
Коды Гоппы, 44
Коды, исправляющие ошибки, 44
Коллизия, 46
Компрометация информации, 43
Контроль доступа, 41
Контроль эффективности защиты информации, 46
Конфиденциальная информация, 42
Конфиденциальность, 41
Концепция защиты информации, 42
Красная книга, 43
Криптоанализ, 42
Криптографическая система, 41
Криптографический протокол, 45
Криптографическое преобразование информации, 45
Криптография, 41
Криптология, 42
Криптосистема Вернама, 46
Криптосистема Габидулина, 46
Криптосистема Крука, 46
Криптосистема МакЭлиса, 46
Криптосистема Нидеррайтера, 46
Криптосистема с временным раскрытием, 45
Криптосистема с открытым ключом, 43
Криптосистема с секретным ключом, 43
Криптосистема с эллиптическими кривыми, 45

Л

Линейный криптоанализ, 48
Лицензиар, 48

Лицензиат, 48
Лицензирование, 48
Лицензия, 48
Логическая бомба, 48
Люк, 48

М

Мандат, 51
Мандатный доступ, 50
Маскарад, 50
Матрица доступа, 51
Метка конфиденциальности, 51
Минимум привилегий, 51
Многоуровневая безопасность, 51
Многоуровневая защита, 51
Многоуровневая криптография, 52
Модель защиты, 52
Модель нарушителя, 52
Монитор ссылок, 51
Морально-этические меры защиты информации, 50

Н

Нарушитель, 53
Национальный Центр Компьютерной Безопасности, 53
Несанкционированное действие, 53
Несанкционированный доступ, 53
Нормы эффективности защиты информации, 53
Носители информации, 53
НСД, 53

О

Обнаружение атак, 54
Обработка информации в АС, 54
Объект, 54
Одноразовая цифровая подпись, 56
Одноразовый блокнот, 56
Односторонняя функция, 55
Односторонняя функция с секретом, 55
Оконечное шифрование, 55
Оранжевая книга, 55
Организационные меры защиты информации, 54
Отказ в обслуживании, 55
Открытое распределение ключей, 55
Открытый ключ, 54
Открытый текст, 54

П

Пароль, 57
Письмо Высшего Арбитражного Суда РФ № С1-7/ОЗ-316, 61
Письмо Высшего Арбитражного Суда РФ № С1-7/ОП-587, 61
План защиты, 57
План обеспечения непрерывной работы и восстановления, 59
Повторное использование объекта, 59
Подотчетность, 58
Подпись кода, 58
Показатель защищенности, 59
Показатель эффективности защиты информации, 60

Полибия квадрат, 59
Политика безопасности, 57
Полномочия, 57
Полномочный доступ, 58
Полный перебор, 60
Пользователь информации, 60
Посредник, 60
Постановление Правительства РСФСР №35, 61
Постановление Правительства РФ №1233, 61
Постановление Правительства РФ №333, 61
Постановление Правительства РФ №608, 61
Потоковый шифр, 58
Потребитель информации, 60
Правила разграничения доступа, 58
Правило доступа, 57
Правило Киркоффа, 59
Право доступа, 57
Правовые меры защиты информации, 58
Привилегии, 57
Протокол отрицания, 60
Протокол с арбитром, 59
Протокол с третьей стороной, 59
Протокол, самообеспечивающий законность, 60
Профиль полномочий, 57

Р

Радужная серия, 62
Разграничение доступа, 62
Разделение секретов, 63
Распознавание атаки, 62
Распределение ключей, 63
Расшифрование, 62
Регистр сдвига с обратной связью, 63
Регламентация, 62
Решение Гостехкомиссии и ФАПСИ №10, 63
Решетка Кардано, 63
Роторная машина, 63
Руководящий документ, 62
Руководящий документ, 64, 65

С

Саями атака, 68
Самопроверяющаяся подпись, 70
Самосинхронизирующаяся потоковая криптосистема, 69
Сборка мусора, 68, 86
Секретный ключ, 70
Сервер-посредник, 70
Сертификат ключа, 70
Сертификат соответствия, 66
Сертификация СЗИ, 66
Синхронизирующаяся потоковая криптосистема, 69
Система анализа защищенности, 66
Система защиты информации, 66
Система криптографической защиты информации, 66
Система обнаружения атак, 66
Скремблер, 67
Скрытые каналы, 68
Скрытый временной канал, 68
Скрытый канал с памятью, 68
Слепая подпись, 70
Сниффинг, 67
Собственник информации, 70
Совершенная секретность, 69
Список аннулированных сертификатов, 70

Список контроля доступа, 68
Спуффинг, 67
Средство защиты информации, 67
Стеганография, 68
Стойкость, 67
Сторнетта-Хабера алгоритм, 68
Субъект, 68
Субъекты информационных отношений, 67
Счетчиковый метод, 69

Т

Технические меры защиты информации, 71
Троянский конь, 71
Туннелирование, 71

У

Угроза АС, 72
Угроза безопасности информации, 72
Угроза интересам субъектов информационных отношений, 72
Указ Президента РФ №188, 73
Указ Президента РФ №334, 73
Управление доступом, 73
Управление ключами, 72
Уровень безопасности, 73
Уровень доступа, 73
Уровень полномочий, 73
Уровень привилегий, 73
Уровень прозрачности, 73
Установление подлинности, 73
Уязвимость АС, 72
Уязвимость информации, 72
Уязвимость субъекта информационных отношений, 72

Ф

ФАПСИ, 74
Федеральное агентство правительственной связи и информации, 74
Физические меры защиты информации, 74

Х

Хагелина машина, 75
Хэш-функция, 75

Ц

Целостность, 76
Цель защиты информации, 76
Центр распределения ключей, 76
Центр сертификации ключей, 76
Цифровая подпись, 76
Цифровой конверт, 77

Ч

Червь, 78

Ш

Шарады Меркля, 79
Шарады с временным замком, 79
Шифр, 79
Шифр Фейстеля, 79
Шифровальные средства, 80
Шифрование, 79
Шифртекст, 79
Шлюз двухпортовый, 80
Шлюз прикладного уровня, 80
Шлюз сеансового уровня, 80

Э

Экран межсетевой, 81
Экран межсетевой с фильтрацией пакетов, 81
Экспоненциальное распределение ключей, 82
Электронная цифровая подпись, 81
Эллиптические кривые, 82
Эль-Гамалы алгоритм, 82
Эффективность защиты информации, 82
ЭЦП, 81

Я

Ядро безопасности, 83