БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
НИИ ПРИКЛАДНЫХ ПРОБЛЕМ МАТЕМАТИКИ И ИНФОРМАТИКИ
ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ
Кафедра математического моделирования и анализа данных

lg0qlqv0cjzsg6j1f69pvelek3dsld1avcwmmhxgfz32aqcrmbm6i8k2tmckndu7
ce4rp1w2bl03khsdan5v02d2qzdgdvirctcxcocm8jmnjf83extn2dcinhgda6oe
nrc4nmjqx43i4huza88if7hpujklxzbb3wj4ovxo530qwq5rbawxatau4dqalhzla
g0855n56z0h3wocddab6n3widnuvf1hm1ilwqfcszbvtwj3sb1t0rperc4k09yxo
d1cl8 07bs
n6njx fbtg6
9qv5t e9rp
g971: zpk9
036k\ dqmx
alewz rfmd1
jg0hicvwpqletgc531nmzpcpb85gceg4ld7681yhktu2cvuwjxrpks8pphkgsos7
o5q481dqsh5u1q829chij1e6rg3w14a86nggdx6cdq5gcow7jppe7t7n8q8jd1
qzwaxyypfveh4vwyh000pbjr0oevlg2taptg285mag6rlx5xq19i6ayx75bcboxoq
r7j1vlv85btzk11qzarsqp4mrlwfasepemswk5ejdcgxci7y14j8htrngpr6cmdwvy
bffksesijisjm2zq5obt2ioiv3mt28jfzzefm83gixh8wzjvjrc20arsks118icia4m8dt
2awmhymh7gtyqfyw8sxiu8b6r4l5da2sxv385fpz4d93mzo0kfbehuyl69jzyjgz
ohhonk2r1ob9e1lefjph2kifft4dt2rn079kcpob8q0e0t3z6srkhw1ffam9vmaquh
kazdsce0wd54lirud2c5vf97ztablebfw2cljrh20prj5254kpuoj95b6t3q44l0mt7
207k249jj72eqigz59jwjg3jew2tu7lah27ubsozghzo8sh3zglg6wjwzlpjeu3u20
c36s1s0askr6xi749zz3xkbhsjgpt4gg5vim6xeybkhhsc5m1ew2h3e3ejyxgoaj
0xsop9af2vsva0ygpw0gyiysokwjxls2wtwnkqmbnyxmtw1gumr68ma49r1uko

СЛОВАРЬ ОСНОВНЫХ ТЕРМИНОВ ПО КРИПТОЛОГИИ

МИНСК
2013

УДК 003.26, 004.056.55
ББК 22.18я73+32.811.4я73
С48

С о с т а в и т е л и:
**Ю. С. Харин, В. В. Герасименок, Г. В. Матвеев,
В. А. Галинский, А. Н. Гайдук**

Рекомендовано советом
факультета прикладной математики и информатики
7 февраля 2013 г., протокол № 4

Р е ц е н з е н т ы :
кафедра информатики Белорусского государственного
университета информатики и радиоэлектроники
(заведующий кафедрой доктор физико-математических наук,
профессор *Л. И. Минченко*);
кафедра «Информационные технологии в управлении»
Белорусского национального технического университета
(заведующий кафедрой доктор технических наук,
профессор *В.Ф. Голиков*)

Словарь основных терминов по криптологии / сост. : Ю. С. Ха-
С48 рин [и др.]. – Минск : БГУ, 2013. – 66 с.

Словарь предназначен для специалистов, занимающихся проектированием, разработкой и эксплуатацией систем и средств криптографической защиты информации, обеспечением мероприятий информационной безопасности в органах государственного и военного управления, банковских и коммерческих структурах, а также для студентов и аспирантов высших учебных заведений, обучающихся по специальностям в области информационной безопасности.

УДК 003.26, 004.056.55
ББК 22.18я73+32.811.4я73

ПРЕДИСЛОВИЕ

Среди способов защиты информации наиболее важным считается криптографический. В последние годы интенсивное развитие телекоммуникационных и информационных систем и расширение круга их пользователей сделали еще более актуальной защиту информации в подобных системах. Кроме традиционных методов криптографической защиты информации на практике стали широко использоваться схемы цифровой подписи, протоколы аутентификации сообщений и абонентов, протоколы распределения ключей и многое другое. Существенное расширение предмета криптографии и круга исследователей и пользователей привело к появлению большого числа новых понятий и терминов, используемых в литературе, научных публикациях и нормативных правовых документах. В результате некоторые термины в различных источниках стали трактоваться по-разному. В ряде случаев имеются различные переводы одного и того же термина с английского языка на русский. Основная цель данного словаря — способствовать формированию единой криптографической терминологии. В контексте словаря слово «секретный» означает понятие «тайный» или «подлежащий сохранению в тайне от не уполномоченных лиц», и не рассматривается в контексте термина «государственные секреты».

При работе над определением термина рассматривались и принимались во внимание несколько литературных источников: книги, словари, журнальные статьи и т.п. В большинстве случаев учитывалось и толкование термина в англоязычных источниках, а окончательный результат являлся, как правило, компромиссом. Использованные в работе источники можно разделить на следующие классы: словари, изданные в России и Украине, монографии по теоретической и прикладной криптографии, учебные пособия, нормативные правовые акты, включая стандарты, связанные с обеспечением безопасности информации. Значительную методическую помощь при работе над терминами и их определениями оказал "Словарь криптографических терминов" под редакцией Б.А. Погорелова, В.Н. Сачкова [25]; в большинстве случаев наши определения и трактовки устоявшихся терминов близки или совпадают с определениями и трактовками, предложенными Б.А. Погореловым, В.Н. Сачковым. Еще одной особенностью словаря является наличие в нем ряда профессиональных терминов, относящихся к практической деятельности в области защиты информации.

В словаре термины упорядочены по алфавиту, причем если термин состоит из нескольких взаимосвязанных слов, то на первое место ставит-

ся существительное, затем идут прилагательные и (или) другие поясняющие слова. Термин выделяется жирным шрифтом, в квадратных скобках приводится соответствующий англоязычный термин и наиболее употребительный синоним. Словарь содержит перекрестные ссылки, которые в тексте выделены курсивом.

Словарь предназначен для специалистов, занимающихся проектированием, разработкой и эксплуатацией систем и средств криптографической защиты информации, обеспечением мероприятий информационной безопасности в органах государственного и военного управления, банковских и коммерческих структурах, а также для студентов и аспирантов высших учебных заведений, обучающихся по специальностям в области информационной безопасности. Представленный словарь предлагается в дальнейшем использовать при разработке Законов Республики Беларусь, государственных стандартов Республики Беларусь и других нормативных правовых актов в области криптографической защиты информации для единой в республике трактовки терминов и определений.

А

Администратор [administrator] — *пользователь*, уполномоченный осуществлять управление информационной системой, и ответственный за ее безопасность и работоспособность.

Администратор безопасности [security administrator] — *пользователь*, уполномоченный осуществлять управление средствами безопасности информационной системы, обеспечивать противодействие потенциальным угрозам, а также ответственный за ликвидацию последствий осуществления угроз.

Аккредитация удостоверяющего центра [certificate authority accreditation] — подтверждение уполномоченным органом компетентности удостоверяющего центра.

Алгоритм выработки кода аутентификации [authentication code generation, син.: режим выработки имитовставки] — вид алгоритма *имитозащиты*, сопоставляющего сообщению *код аутентификации*. Алгоритм принятия решения о подлинности сообщения основан на проверке значения *кода аутентификации* сообщения. К а. в. к. а. предъявляются требования: невозможность вычисления *кода аутентификации* для заданного сообщения без знания *ключа*; невозможность подбора для одного или нескольких сообщений с известными значениями *кода аутентификации* нового сообщения с заданным значением *кода аутентификации* без знания *ключа*.

Алгоритм выработки ЭЦП [signature generation, син.: алгоритм формирования (генерации) подписи цифровой (ЭЦП)] — *алгоритм криптографический* вычисления *подписи электронной цифровой* сообщения с использованием *ключа секретного* **(**личного), являющийся составной частью *системы (схемы) подписи цифровой*. Алгоритм (вообще говоря, рандомизированный), на вход которого подаются подписываемое сообщение, *ключ секретный,* а также открытые параметры *схемы подписи цифровой*. Результатом работы алгоритма является *подпись электронная цифровая.*

Алгоритм зашифрования [encryption algorithm, син.: зашифрование] — *алгоритм криптографический*, реализующий функцию *зашиф-*

рования.

Алгоритм криптографический [cryptographic algorithm, син.: криптоалгоритм, алгоритм криптографического преобразования, криптографическое преобразование, криптопреобразование] — алгоритм, реализующий одну из *функций криптографических*.

Алгоритм криптографический асимметричный [asymmetric cryptographic algorithm] — включает *алгоритм шифрования асимметричный* и *схему ЭЦП*. А. к. а. использует асимметричную пару ключей*: ключ открытый* и *ключ личный.*

Алгоритм проверки ЭЦП [signature verification] — составная часть *схемы подписи цифровой.* Алгоритм, на вход которого подаются *подпись цифровая, ключ открытый* и другие открытые параметры схемы подписи цифровой. В схемах *подписи цифровой* с восстановлением сообщения результатом работы алгоритма является заключение о корректности подписи и, если она корректна, то само сообщение, извлеченное из подписи. В остальных случаях сообщение является частью входных данных, и алгоритм проверки выдает лишь заключение о корректности подписи.

Алгоритм расшифрования [decryption algorithm, син.: расшифрование] — *алгоритм криптографический*, реализующий функцию *расшифрования*.

Алгоритм хэширования [hashing algorithm] — алгоритм вычисления значения *хэш-функции криптографической*.

Алгоритм шифрования [ciphering algorithm] — общее название *алгоритма зашифрования* и *алгоритма расшифрования*.

Алгоритм шифрования асимметричный [asymmetric encryption algorithm, public-key encryption, син.: асимметричное шифрование] — алгоритм шифрования, в котором *зашифрование* осуществляется с помощью *ключа открытого*, а *расшифрование* с помощью *ключа секретного* (личного), функционально связанного с *ключом открытым*. *Стойкость криптографическая* а. ш. а. определяется трудоемкостью, с которой *противник* может вычислить *ключ секретный*, исходя из знания *ключа открытого* и другой дополнительной информации об а. ш. а.

Алгоритм шифрования блочный [block encryption, block cipher, син.: блочное шифрование] — *алгоритм шифрования симметричный*, в котором *функция шифрования* преобразует блоки *текста открытого* в блоки *шифртекста*, как правило, той же фиксированной длины.

Алгоритм шифрования поточный [stream cipher, син.: поточное шифрование] — *алгоритм шифрования симметричный*, в котором функция шифрования преобразует *текст открытый* в *шифртекст*, посимвольно, например, с использованием соответствующих символов *гаммы*.

Алгоритм шифрования симметричный [symmetric encryption algorithm, син.: симметричное шифрование] — алгоритм шифрования, в котором *зашифрование* и *расшифрование* осуществляется с помощью одного и того же *ключа секретного*. *Стойкость криптографическая* а. ш. с. определяется трудоемкостью, с которой *противник* может вычислить *ключ секретный*, исходя из допущения о полноте знания *противником* а. ш. с. с точностью до *ключа секретного*.

Алфавит [alphabet] — множество символов, используемое для кодирования (представления) данных.

Анализ криптографический [cryptanalysis, син.: криптоанализ] — раздел прикладной математики и информатики, изучающий модели, методы, алгоритмы, программные и аппаратные средства анализа *криптографических протоколов, криптографических алгоритмов, криптосистем* или их входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая открытый текст, а также получения обоснованных оценок их *стойкости криптографической*.

Анонимность [anonymity] — возможность участников *протокола* выполнять какие-либо операции анонимно, т.е. без присваивания им уникальных идентификаторов и удостоверения их подлинности.

Аппаратные средства [hardware means] — см. *средства аппаратые*.

Аппаратура линейного шифрования [син.: аппаратура засекречивания, засекречивающая аппаратура связи (ЗАС)] — вид *аппаратуры шифровальной*, предназначенный для *зашифрования* информации непосредственно при ее передаче по *каналу связи* и *расшифрования* информа-

ции, получаемой по *каналу связи*.

Аппаратура предварительного шифрования [preliminary enciphering facility] — вид *аппаратуры шифровальной*, в которой процесс *шифрования* информации разнесен по времени с процессом ее передачи по системам электросвязи.

Аппаратура шифровальная [cryptographic hardware, enciphering hardware, encryption hardware, син.: аппаратура шифрования, шифровальная аппаратура] — см. *аппаратура шифрованния*.

Аппаратура шифрования [cryptographic hardware, enciphering hardware, encryption hardware, син.: шифровальная аппаратура] — вид аппаратуры, предназначенный для обеспечения *конфиденциальности* информации, содержащей государственные секреты, передаваемой по линиям (сетям) электросвязи за пределы контролируемой зоны. К а. ш. относятся: *аппаратура предварительного шифрования*, *аппаратура линейного шифрования*, аппаратура изготовления *ключевых документов* к а. ш. А. ш. относится к *средствам криптографической защиты государственных секретов*. Особенностью а. ш. является то, что *информацию,* содержащую государственные секреты, зашифрованную с применением а. ш. можно передавать по открытым *каналам связи*, в том числе и за пределы контролируемой зоны.

Арбитр [arbiter] — участник *протокола* с арбитром, выполняющий процедуру *арбитража*.

Арбитраж [arbitration] — формализованная процедура разрешения споров о трактовке результатов выполнения *протокола криптографического.* Такая процедура необходима для многих *протоколов криптографических* прикладных, в т.ч. *схем подписи цифровой, протоколов* подписания контракта, систем платежей электронных и т.п., и должна рассматриваться как неотъемлемая часть этих *протоколов*. Для самой процедуры арбитража требуется либо алгоритм, выполняемый арбитром на входных данных, предоставленных ему заявителем (заявителями), либо специальный *протокол* с участием всех заинтересованных сторон.

Атака адаптивная [adaptive attack] — атака на *криптосистему*, при которой характер воздействия *противника* и/или *нарушителя* может изменяться во времени в зависимости от действий *пользователей крипто-*

системы или от других условий. Например, *противник* может подбирать различные исходные данные для воздействия на *криптосистему*.

Атака активная [active attack] — атака на *криптосистему* или на *протокол криптографический*, при которой *противник* и/или *нарушитель* может влиять на действия *пользователя*, например, подменять или удалять сообщения *пользователя* законного, создавать и передавать сообщения от его имени и т. п.

Атака «встреча посередине» [meet-in-the-middle attack] — атака на *криптосистему*, основанная на *методе «встреча посередине»*.

Атака дифференциальная [differential attack, син.: атака разностная] — атака на *криптосистему*, основанная на *методе разностном*.

Атака дифференциально-линейная [differential-linear attack, син.: атака разностно-линейная] — см. *атака разностно-линейная*.

Атака корреляционная [correlation attack] — атака на *криптосистему*, основанная на *методе корреляционном*.

Атака линейная [linear attack] — атака на *криптосистему*, основанная на *методе линейном*.

Атака на криптосистему [attack on the cryptosystem] — попытка реализации *угрозы* информационной безопасности *противником* и/или *нарушителем*.

Атака на криптосистему на основе известного текста открытого [known plaintext attack] — атака на *криптосистему*, при которой *противнику* и/или *нарушителю* известен *текст открытый*.

Атака на криптосистему на основе текста шифрованного [ciphertext-only attack] — атака на *криптосистему*, при которой *противнику* и/или *нарушителю* известен *текст шифрованный* и не известен *текст открытый*.

Атака на основе ключей эквивалентных [equivalent keys attack] — атака на *криптосистему*, основанная на возможности объединения *ключей криптосистемы* в классы эквивалентности и опробования только

одного ключа из каждого класса.

Атака на протокол криптографический [attack on the protocol] — попытка проведения анализа сообщений *протокола* и/или выполнения не предусмотренных *протоколом* действий с целью нарушения работы *протокола* и/или получения информации, составляющей секрет его участников.

Атака пассивная [passive attack] — атака на *криптосистему* или *протокол криптографический*, при которой *противник* и/или *нарушитель* наблюдает и использует передаваемые *сообщения шифрованные*, но не влияет на действия *пользователей* и не изменяет состояние *криптосистемы*.

Атака полного перебора [brute-force attack, син.: атака тотального перебора, атака грубой силы] — *атака* на *криптосистему*, основанная на *методе полного (тотального) опробования ключей*.

Атака «противник в середине» [man-in-the-middle attack] — *атака на протокол криптографический*, в которой противник С выполняет этот *протокол* как с участником А, так и с участником В. Противник С выполняет сеанс с участником А от имени В, а с участником В — от имени А. В процессе выполнения противник пересылает сообщения от А к В и обратно, возможно, подменяя их (отсюда название атаки). В частности, в случае *протокола аутентификации* абонента успешное осуществление атаки «противник в середине» позволяет противнику аутентифицировать себя для В под именем А. Для осуществления атаки «противник в середине» необходимо обеспечивать синхронизацию двух сеансов *протокола*.

Атака с повторной передачей [reply attack] — *атака на протокол криптографический*, при которой *противник* и/или *нарушитель* записывает все передаваемые сообщения и впоследствии повторно передает их от имени *пользователя*.

Атака разностная [differential attack, син.: атака дифференциальная] — атака на *криптосистему*, основанная на *методе разностном*.

Атака разностно-линейная [differential-linear attack, син.: атака дифференциально-линейная] — *атака* на *криптосистему*, основанная

на *методе разностно-линейном*.

Атака со словарем [dictionary attack] — атака на *криптосистему*, использующая словарь в некотором конечном *алфавите*.

Аудит безопасности ИОК [PKI audit] — периодический, независимый и документированный процесс проверки выполнения субъектами *инфраструктуры открытых ключей* (ИОК) политики ИОК в области безопасности.

Аудит информационной безопасности [information security audit] — периодический, независимый и документированный процесс проверки выполнения установленных требований по обеспечению информационной безопасности.

Аутентификация [authentication] — проверка и подтверждение подлинности различных аспектов информационного взаимодействия: источника передаваемых сообщений, *пользователя*, сеанса связи, времени взаимодействия и т. д. В конкретных случаях используются следующие уточняющие термины: аутентификация абонента (*пользователя*) [user authentication], *аутентификация взаимная* [mutual authentication], аутентификация интерактивная [interactive authentication], аутентификация источника данных [data origin authentication], *аутентификация односторонняя* [one-way authentication], аутентификация сторон [entity authentication]. Аутентификация обычно осуществляется перед выдачей разрешения на доступ.

Аутентификация взаимная [mutual authentication] — вариант *аутентификации сторон,* при котором каждая из сторон проверяет, что взаимодействующая с ней сторона — именно та, за которую себя выдает. А. в. реализуется таким *протоколом идентификации,* в котором каждый из *участников* является одновременно и доказывающим, и проверяющим. Это позволяет за один сеанс выполнения *протокола* каждым из участников доказать другому участнику свою идентичность.

Аутентификация односторонняя [one-way authentication] — *аутентификация сторон,* при которой одна из сторон проверяет, что взаимодействующая с ней сторона - именно та, за которую себя выдает. А. о. реализуется *протоколом идентификации* с двумя участниками: доказывающим и проверяющим. Термин «односторонняя» используют, чтобы

отличить ее от *аутентификации взаимной.*

Б

Батарея тестов статистических [battery of statistical tests] — система *тестов статистических* для проверки некоторой нулевой гипотезы 1 (например, гипотезы о равномерно распределенной случайной последовательности) против ряда альтернатив $H_1, H_2, \ldots, H_N$ (например, альтернативы о неравномерном распределении вероятностей, альтернативы о марковской зависимости) на основе выходной последовательности *системы криптографической*. Примеры б. т.: батарея Д.Кнута (9 тестов); батарея Дж. Марсальи (18 тестов); батарея NIST (15 тестов); батарея CRYPT-X (13 тестов).

S-блок [S-box, substitution-box] — *примитив криптографический*, являющийся составной частью большинства *алгоритмов симметричного шифрования*, который преобразует *m* входных бит в *n* выходных, где *m* и *n* не обязательно равны. Поэтому его можно задать с помощью некоторой таблицы называемой S-блоком. S-блок должен удовлетворять ряду критериев для усложнения степени зависимости *шифртекста* от *ключа*.

Блок текста [text block] — *последовательность*, составленная из *m* подряд идущих знаков *текста открытого,* промежуточного или *шифртекста*. Обычно текст разбивается на блоки одинаковой длины *m* — непересекающиеся *m*-граммы.

В

Верификация [verification] — доказательство соответствия или несоответствия предмета верификации его формальному описанию. Предметом могут выступать алгоритмы, программы и другие объекты.

Вектор инициализации [initialization vector] — вектор, который передается по каналу управления и используется для инициализации *алгоритма шифрования*. См. также *синхропосылка*.

Верификация маршрута сертификации [certification path validation] — заключается в *верификации* всех *цифровых подписей* на

сертификатах, составляющих путь сертификации, определении периода действия каждого сертификата и статуса каждого сертификата, а также в отслеживании ограничений на имена и т.д.

Владелец сертификата открытого ключа [certificate holder's public key] — физическое или юридическое лицо, осуществившее выработку *личного* (*секретного*) *ключа* и соответствующего ему *открытого ключа*, на имя которого *удостоверяющим центром* выдан *сертификат открытого ключа*.

Г

Гамма [keystream, ciphering sequence, key sequence] — *последовательность* символов *алфавита*, используемая в шифрсистемах поточных, реализующих гаммирование. Для обеспечения *стойкости криптографической* г. должна удовлетворять ряду требований, в частности, быть близкой по своим свойствам к реализации *последовательности случайной равномерно распределенной* (чисто случайной).

Генератор последовательностей псевдослучайных [pseudorandom generator] — техническое устройство или программа для выработки *последовательностей псевдослучайных*.

Генератор программный [software generator] — программа имитации на компьютере реализации последовательности случайной равномерно распределенной.

Генератор РРСП [randomnumber generator] — устройство, позволяющее по запросу получить реализацию *последовательности случайной равномерно распределенной* (чисто случайной). Выделяют три типа генераторов РРСП: табличный, физический и программный.

Генератор случайных чисел [randomnumber generator] — программа или устройство, предназначенные для выработки последовательности псевдослучайных чисел по заданному закону распределения.

Генератор табличный [table generator] — генератор РРСП, который в качестве источника случайных чисел использует специальным образом составленные таблицы, содержащие проверенные, не зависящие друг от

друга цифры.

Генератор физический [hardware generator] — генератор РРСП, удовлетворяющий требованиям технических нормативных правовых актов по безопасности информации и использующий в качестве источника случайных чисел физический шум, например, детекторы событий ионизирующей радиации, дробовой шум в резисторе или космическое излучение.

Генерация ключей [key generation] — последовательность действий, описанная в технологическом процессе, определяющая порядок выпуска *документов ключевых* на аппаратуре изготовления ключей, а также порядок создания ключей в *аппаратуре шифровальной* с использованием *генераторов РРСП*.

Государственная система шифрованной связи [national public security communication system] — см. *система шифрованной связи государственная*.

m-грамма [m-gram, син.: мультиграмма] — фрагмент текста, состоящий из m последовательно идущих символов, т.е. элемент множества A^m, где A — *алфавит*.

Граница криптографическая [cryptographic boundary, син.: криптографическая граница] — точно определенный замкнутый периметр, охватывающий *модуль криптографический* и очерчивающий его физические границы.

Д

Дешифрование [breaking of cryptosystem] — процесс аналитического раскрытия *противником* и/или *нарушителем сообщения открытого* без предварительного полного знания всех элементов *системы криптографической*. Если этот процесс поддается математической формализации, говорят об алгоритме дешифрования.

Доказательство знания [proof of knowledge, син.: протокол доказательства знания] — *доказательство интерактивное,* при котором доказывающий убеждает проверяющего в том, что он владеет секретной

информацией, не раскрывая её.

Доказательство интерактивное [interactive proof] — понятие теории сложности вычислений, составляющее основу понятия *доказательства с разглашением нулевым.* Д. и. — оказательство путем выполнения *протокола* с двумя *участниками,* доказывающим и проверяющим, в процессе работы которых участники обмениваются сообщениями (запросы и ответы), обычно зависящими от случайных чисел, которые могут содержаться в секрете. Цель доказывающего — убедить проверяющего в истинности некоторого утверждения. Проверяющий либо принимает, либо отвергает доказательство. В отличие от обычного математического понятия доказательства в данном случае доказательство носит не абсолютный, а вероятностный характер и характеризуется двумя вероятностями. Если доказываемое утверждение верно, то доказательство должно быть верным с вероятностью, стремящейся к единице при увеличении числа циклов *протокола.* Если же доказываемое утверждение ложно, то при увеличении числа циклов *протокола* вероятность правильности доказательства должна стремиться к нулю. Криптографическое качество *протокола* д. и. характеризуется свойствами *полноты,* корректности и *разглашения нулевого.*

Доказательство не интерактивное с разглашением нулевым [noninteractive zero-knowledge proof] — *доказательство с разглашением нулевым,* выполняемое за один цикл (*протокола*)*:* доказывающий посылает сообщение проверяющему, который на основе анализа этого сообщения либо принимает, либо отвергает доказательство.

Доказательство с разглашением нулевым [zero-knowledge proof] — *доказательство знания,* которое обладает свойством *разглашения нулевого.*

Доказательство с разглашением нулевым совершенное [perfect zero-knowledge proof] — предельный случай *доказательства с разглашением нулевым,* в котором количество дополнительной информации, которую может получить проверяющий в результате выполнения *протокола,* равно нулю.

Документ ключевой [key document] — физический носитель определенной структуры, содержащий ключевую информацию.

Документ электронный [electronic document] — документ в электронном виде с реквизитами, позволяющими установить его целостность и подлинность.

З

Зашифрование [encryption, enciphering, син.: функция зашифрования] — математическое преобразование *сообщения открытого x* в *сообщение шифрованное y* с помощью функции зашифрования $f_k : x \to y$, зависящей от ключа зашифрования *k*, принимающего значения из некоторого *множества ключевого*.

Защита информации криптографическая [cryptographic providing of information security] — *защита информации* при помощи средств *криптографической защиты информации*.

И

Идентификация [identification] — процедура присвоения данной стороне уникального системного имени – идентификатора, которое позволяет отличать ее от других сторон. Обычно процедура и. заключается в предъявлении этого имени и предшествует *аутентификации*.

Избыточность (языка) [redundancy of language] — теоретико-информационная характеристика языка $r = h_+ - h \geq 0$, где $h_+ = \log_2 N$ — максимально возможная энтропия (на один символ) для алфавита данного языка, N — число символов в алфавите, а h - статистическая оценка энтропии (на один символ) для сообщений данного языка. Например, согласно [47] для английского языка $N = 26$, $r = 3.4$ бита на символ.

Имитовставка [message authentication code] — см. *код аутентификации сообщения.*

Имитозащита [integrity protection, protection from imitation] — защита сообщений в *системе криптографической* от навязывания ложных данных путем добавления к зашифрованным данным *имитовставки.*

Имитостойкость [imitation resistance] — свойство *системы криптографической* или *протокола*, характеризующая стойкость к атакам со стороны *противника* и/или *нарушителя*, целью которых является навязывание ложного сообщения, подмена передаваемого сообщения или изменение хранимых данных.

Информация [information] — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информация критическая [sensitive information] — см. *объект критический*.

Инфраструктура открытых ключей (ИОК) [public key infrastructure, PKI] — подсистема *системы ключевой шифрсистемы асимметричной.* Предназначена для обеспечения (с помощью *сертификатов ключей)* доверия *пользователей* к подлинности *ключей,* соответствия *ключей пользователям* и оговоренным условиям их применения.

ИОК корпоративная [corporation PKI] — ИОК корпоративной информационной системы. *Удостоверяющий центр* корпоративной ИОК может издавать *самоподписанный сертификат*, если это предусмотрено политикой безопасности корпоративной ИОК.

Использование гаммы повторное [reusing the same keystream twice] — событие, состоящее в том, что шифровальщик вследствие ошибочных действий для *зашифрования* различных данных использовал один и тот же *ключ* в *криптографической системе*, реализующей гаммирование.

К

Канал связи [communication channel] — совокупность технических средств, процессов и политик, определяющих передачу зашифрованной *информации* между *аппаратурой шифровальной*.

Канал связи квантовый [quantum communication channel] — *канал связи* для передачи *информации*, основанный на принципах квантовой физики.

Ключ [key] — изменяемый элемент (параметр), каждому значению ко-

торого однозначно соответствует одно из *криптопреобразований*, реализуемых к*риптосистемой*. Все возможные значения ключа составляют *множество ключевое криптосистемы.*

Ключ главный [master key] — *ключ*, который используется для шифрования *ключей шифрования ключей*, предназначенных для *шифрования ключей разовых* или для генерации других видов *ключей* посредством *шифрования* определённых данных.

Ключ долговременный [long-term key] — *ключ,* действующий в неизменном виде длительное время.

Ключ зашифрования [enciphering key] — *ключ*, используемый при з*ашифровании*.

Ключ личный [private key] — *ключ* (секретный) асимметричной пары ключей *алгоритма криптографического асимметричного*, который может быть использован только его владельцем (объектом) и должен сохраняться в тайне.

Ключ открытый [public key] — несекретный *ключ* асимметричной пары ключей *алгоритма криптографического асимметричного*.

Ключ разовый [once-only key] — *ключ*, однократно используемый для *шифрования* в жизненном цикле ключей.

Ключ расшифрования [decryption key] — *ключ*, используемый при *расшифровании*.

Ключ сеансовый [session key] — *ключ*, специально сгенерированный для одного сеанса связи между двумя участниками.

Ключ секретный [secret key] — *ключ*, сохраняемый в секрете от лиц, не имеющих допуска к ключам данной *криптосистемы* симметричной или к использованию некоторых функций данной *криптосистемы* асимметричной.

Ключ скомпрометированный [compromised key] — *ключ секретный*, ставший доступным лицам, не имеющим допуска к *ключам* данной *криптосистемы* симметричной или к использованию некоторых функ-

ций данной *криптосистемы* асимметричной.

Ключ слабый [weak key] — *ключ криптосистемы*, при котором заметно ухудшаются характеристики *стойкости криптографической криптосистемы* по сравнению со средними значениями тех же характеристик при *ключе*, случайно равновероятно выбранном из *множества ключевого криптосистемы*.

Ключ цикловой (раундовый) [round key, син.: раундовый ключ] — *ключ*, вычисляемый по *ключу секретному алгоритма шифрования*. Используется для преобразования блока *информации* на одном из циклов (раундов) *шифрования*.

Ключ шифрования данных [data encryption key] — *ключ*, предназначенный для *шифрования* данных.

Ключ шифрования ключей [key enciphering key (KEK)] — *ключ*, используемый для *шифрования ключей разовых*.

Ключи эквивалентные [equivalent keys] — *ключи*, при которых *криптосистема* реализует одинаковые отображения.

Ключевой документ [key document] — см. *документ ключевой*.

Код аутентификации [message authentication code, seal, integrity check value, син.: имитовставка] — в *протоколах аутентификации сообщений* с доверяющими друг другу участниками — специальный набор символов, добавляемый к сообщению и предназначенный для обеспечения его *целостности* и *аутентификации* источника данных.

Коллизия [collision, existential collision] — событие, при котором значения *хэш-функции* от разных сообщений совпадают.

Количество информации по Шеннону [Shannon's information] — количеством информации $I(A/B)$, которое заключено в случайном событии (сообщении) B относительно A, называется число $I(A/B) = \log \frac{P(A/B)}{P(A)}$, где $P(\cdot)$ — вероятность. Число $I(A/A)$ называется количеством информации, заключающейся в событии A: $I(A/A) = I(A) = -\log P(A)$.

Компрометация [compromise] — случай утраты, разглашения, кражи, несанкционированного копирования и т.п. ключевых данных и *средств криптографической защиты*, который может привести или привел к утечке информации о них.

Компрометация абонента [compromise of a party] — факт ознакомления *противника* и/или *нарушителя* с *ключами секретными* абонента защищенной информационной сети. Может иметь явный или тайный характер.

Компрометация ключа [compromise of a key] — событие, в результате которого *ключ* может стать известным посторонним лицам.

Компрометация аппаратуры шифровальной [compromise of cryptographic hardware] — утеря или хищение *аппаратуры шифровальной*, несанкционированная передача ее третим лицам, ознакомление с ней лиц, не имеющих установленного допуска к этим средствам, а также разглашение сведений о ней.

Компрометация шифрсистемы [compromise of a cryptosystem] — событие, в результате которого секретные *криптографические алгоритмы* и *протоколы*, используемые в шифрсистеме, могут стать известными посторонним лицам.

Конфиденциальность [confidentiality, privacy] — свойство *информации*, означающее, что она предназначена только определенному кругу лиц, хранится в тайне от всех остальных и ее использование неавторизованными лицами может стать причиной ущерба для организации. Как правило, эта *информация* составляет служебную, профессиональную, промышленную, коммерческую или иную тайну.

Кроссертификация [cross certification] — процедура изготовления специальных *сертификатов открытых ключей* независимых *центров удостоверяющих* (кроссертификатов) для взаимодействия *владельцев сертификатов открытых ключей*, изготовленных данными *центрами удостоверяющими*.

Кривая эллиптическая [elliptic curve] — это алгебраическая кривая над

полем F, заданная уравнением Вейерштрасса: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, где $a_{1,}a_{2,}a_{3,}a_{4,}a_6 \in F$, вместе с точкой на бесконечности. Эллиптические кривые являются одним из основных объектов изучения в современной теории чисел и *криптографии*. *Криптография* с использованием эллиптических кривых образует самостоятельный раздел *криптографии*. В частности, на эллиптических кривых основаны многие стандарты *цифровой подписи*.

Криптоаналитик [cryptanalyst] — специалист, занимающийся *криптоанализом систем криптографических*.

Криптограмма [cryptogram] — *сообщение зашифрованное*, оформленное по действующим правилам пользования *системой шифрования*. Содержит, кроме текста шифрованного, адрес, грифы срочности и др. служебную *информацию*.

Криптография [cryptography] — область научных, прикладных, инженерно-технических исследований и практической деятельности, которая связана с разработкой *средств криптографической защиты информации* от *угроз* со стороны *противника* и/или *нарушителя* и обоснованием их *стойкости криптографической.* В настоящее время основными задачами к. являются обеспечение *конфиденциальности, целостности, аутентификации,* невозможности отказа, неотслеживаемости. В отличие от организационных и других способов защиты *информации*, под криптографическими понимаются такие, которые используют математические и компьютерные (электронные) методы преобразования защищаемой *информации*.

Криптология [cryptology] — общее название *криптографии* и *криптоанализа.*

Криптопреобразование [cryptographical transformation, син.: функция криптографическая] — см. *функция криптографическая*.

Криптосистема с открытым ключом [public-key cryptosystem, asymmetric cryptosystem, public-key encryption, син.: алгоритм шифрования асимметричный] — см. *алгоритм шифрования асимметричный*.

RSA-криптосистема [RSA encryption algorithm, the RSA cryptosystem] — *криптосистема с открытым ключом*, используемая

как для *шифрования*, так и для *цифровой подписи. Алгоритмы зашифрования* и *расшифрования* основаны на возведении в степень в кольце вычетов по модулю, являющемуся произведением двух больших простых чисел, а ее стойкость напрямую связана с предполагаемой сложностью задачи факторизации целого числа. Предложена в 1978 году Р. Райвестом, А.Шамиром и Л. Адлеманом.

Криптосистема Рабина [the Rabin cryptosystem] — *криптосистема* с *открытым ключом,* основанная на операции возведения в квадрат по модулю, являющемуся произведением двух больших простых чисел. Ее стойкость связана с трудностью извлечения квадратного корня по этому модулю. Более того, строго доказано, что извлечение квадратного корня эквивалентно факторизации модуля.

Криптосистема Эль-Гамаля [the ElGamal cryptosystem] — *криптосистема с открытым ключом*, основанная на трудности вычисления дискретного логарифма. *Криптосистему* можно использовать для *шифрования* и *цифровой подписи*. Схема Эль-Гамаля лежит в основе *стандарта электронной цифровой подписи* России.

Л

Линия связи [communication line, communication link] — линия передачи, физические цепи и линейно – кабельные сооружения, используемые для передачи данных между *аппаратурой шифровальной*.

М

Маркант [син.: ключевые группы] — условные группы, проставляемые в исходной *криптограмме*, с помощью которых по установленным правилам определяется *ключ разовый* для данной *системы ключевой*, использованный при *зашифровании* соответствующей исходной шифртелеграммы.

Маршрут сертификации [certification path, син.: путь сертификации] — упорядоченная последовательность сертификатов, которая может быть обработана вместе с *открытым ключом* начального объекта для признания *открытого ключа* конечного объекта.

Метод анализа криптографического [crypt-analytic method, method of cryptanalysis, син.: метод криптоанализа] — последовательность действий, направленная на исследование *стойкости криптографической криптосистемы*, объединенных одной или несколькими идеями (математическими, техническими или другими). Можно предположить, что и разработчик криптосистем, и *противник* и/или *нарушитель* используют одну и ту же совокупность м. а. к. В качестве наиболее важных характеристик м. а. к. обычно рассматривают трудоемкость м. а. к. и надежность м. а. к.

Метод «встреча посередине» [meet-in-the-middle attack] — *метод анализа криптографического*, состоящий из двух этапов. Первоначально *ключ* разбивается на две части, на первом этапе производятся вычисления для одной части *ключа*, результаты которых записываются в память, на втором этапе определяется *ключ* путем последовательного обращения к памяти.

Метод дифференциальный [differential cryptanalysis] — см. *метод разностный*.

Метод дифференциально-линейный [differential-linear cryptanalysis] — см. *метод разностно-линейный*.

Метод коллизий [cryptanalysis based on collision search] — *метод анализа криптографического*, основанный на возможности (при определенных условиях) использования *коллизий*.

Метод корреляционный [correlation cryptanalysis] — *метод анализа криптографического*, использующий статистические зависимости между внутренними состояниями *криптосистемы* (как автомата) и значениями входной и выходной последовательностей.

Метод линейный [linear cryptanalysis] — *метод анализа криптографического*, основанный на замене нелинейных соотношений (уравнений) относительно неизвестного параметра линейными. Важную роль при этом играет вероятность с которой выполняется данное линейное соотношение. Различают разновидности метода для шифрсистем поточных и шифрсистем блочных.

Метод на основе парадокса дней рождения [birthday attack] — *метод анализа криптографического*, основанный на использовании *парадокса дней рождения*.

Метод полного (тотального) опробования ключей [exhaustive key search, brute-force attack] — *метод анализа криптографического*, состоящий в переборе всех возможных *ключей криптосистемы* с отбраковкой ложных вариантов по некоторому критерию.

Метод протяжки вероятного слова [moving probable word cryptanalysis] — *метод анализа криптографического*, состоящий в последовательном опробовании места в *тексте шифрованном*, соответствующего вероятному фрагменту *текста открытого*. При истинном варианте опробования возможно составление и решение уравнений относительно неизвестного *ключа*.

Метод частичного опробования ключа [sequential key search] — *метод анализа криптографического*, состоящий в последовательном опробовании и отбраковке *ключей криптосистемы* в соответствии с некоторыми упорядочениями на множестве *ключей*. Как правило, применяются специально подобранные упорядочения *множества ключевого*, например, с учетом вероятностей появления *ключей.*

Метод разностный [differential cryptanalysis] — *метод анализа криптографического*, заключающийся в выборе метрики разности и анализе влияния разности между блоками *текста открытого* на разность блоков *текста шифрованного*. Имеет ряд модификаций, например, усеченный, метод бумеранга и др.

Метод разностно-линейный [differential-linear cryptanalysis, син.: метод дифференциально-линейный] — *метод анализа криптографического*, объединяющий *метод разностный* и *метод линейный*.

Метрика Хэмминга [Hamming metric] — метрика, определенная на множестве векторов одинаковой длины и равная *расстоянию Хэмминга* между парами векторов.

Многочлен неприводимый [irreducible polinomial] — многочлен ненулевой степени, который не имеет делителей меньшей положительной степени. В случае конечного поля F_q число неприводимых многочленов

степени n со старшим коэффициентом равным единице, вычисляется по формуле $N_q(n) = \frac{1}{n}\sum_{d|n}\mu(\frac{n}{d})q^d$, где $\mu(x)$ — функция Мебиуса.

Многочлен примитивный [primitive polynomial] — неприводимый многочлен над полем Галуа F_q степени m и старшим коэффициентом равным единице, корень которого порождает мультипликативную группу поля F_{q^m}.

Множество ключевое (криптосистемы) [key set (of a cryptosystem)] — множество всех возможных значений *ключа криптосистемы*.

Модуль криптографический [cryptographic module, син.: криптографический модуль] — набор технических, программных, аппаратно-технических средств или любая их комбинация, в которых реализованы *функции криптографические* и/или генерация (хранение) ключевых данных.

Н

Нарушитель [adversary, син.: противник] — субъект, реализующий *угрозы* информационной безопасности.

Носитель ключа [key carrier, син.: ключевой носитель] — физический носитель, предназначенный для хранения ключевой *информации*.

О

Оборудование шифрованной связи [security carrier, син.: оборудование засекреченной связи] — технические средства, взаимодействующие с *аппаратурой шифровальной* или управляющие ею, которые могут влиять на *стойкость криптографическую*.

Объект криптографический [cryptographic object, син.: криптографический объект] — *критические* и *открытые объекты системы криптографической*.

Объект информационный [data entity] — описание субъекта (субъектов) и (или) объекта (объектов) информационных отношений в государственных информационных ресурсах исходя из назначения государственных информационных ресурсов.

Объект критический [sensitive objects, син.: критическая информация] — *информация*, *компрометация* или нарушение *целостности* которой может привести к снижению *уровня безопасности системы криптографической*.

Объект открытый [public object] — *информация*, за исключением критической, нарушение *целостности* которой может привести к снижению *уровня безопасности системы криптографической*.

Оператор [operator] — *пользователь*, осуществляющий эксплуатацию информационной системы в пределах своих прав доступа.

Орган шифровальный [encryption department, син.: шифровальный орган] — самостоятельный объект (отделение, подразделение, пост специальной связи, группа), включающий кадровый личный состав, штатную *аппаратуру шифрования*, *оборудование засекреченной связи* и вспомогательное оборудование (материалы), размещённые в стационарных помещениях или на подвижных объектах.

Отображение, не распространяющее искажений [mapping free of error propagation, син.: отображение, не размножающее искажений] — отображение множества всех слов конечных длин в одном *алфавите* во множество всех слов конечных длин в другом *алфавите*, сохраняющее длину слов и для которого *расстояние Хэмминга* между образами любых слов одинаковой длины не превосходит *расстояния Хэмминга* между исходными словами.

Отображение некоррелированное [uncorrelated mapping] — отображение: $f : X^n \to X^m$, для которого при случайном равновероятном выборе аргументов $x \in X^n$ совместное распределение *j*-ой координатной функции отображения *f(x)* и *i*-й координаты аргумента *x* является равномерным на X^2 для всех $i \in (1,...,n)$ и всех $j \in (1,...,m)$.

Отображение сбалансированное [balanced mapping, син.: отображе-

ние равновероятное] — отображение: $f : X^m \to X^n$, для которого при всех $x \in X^n$ мощности полных прообразов $f^{-1}(x)$ одинаковы.

Отображение равновероятное [balanced mapping] — см. *отображение сбалансированное.*

П

Парадокс дней рождения [birthday paradox] — свойство выборки из *t* независимых случайных знаков *n*-элементного *алфавита*, состоящее в том, что вероятность появления в выборке двух одинаковых знаков не меньше $1-e^{-a}$, если $C_t^2 > na > 0$. П. д. р. используется в *криптографии* для оценки различных характеристик *криптосистем*, например, для оценки длины *текста шифрованного*, позволяющего составить уравнения относительно неизвестного *ключа*.

Параметр криптографического преобразования [critical security parameter, син.: криптографический параметр] — изменяемый элемент *функции криптографической*, каждому значению которого соответствует одно из преобразований, реализуемое *функцией криптографической*. В отличии от *ключа*, который обычно держится в секрете, п. к. п., как правило, является известным элементом *функции криптографической*.

Пароль [password] — последовательность символов, используемая для *аутентификации* уполномоченных *пользователей* и известная только уполномоченным *пользователям*. Часто пароли обладают лингвистическими особенностями, способствующими их запоминанию, однако это позволяет *противнику* и/или *нарушителю* проводить эффективные *атаки со словарем*.

Подделка подписи цифровой [forgery] — реализация атаки на систему *подписи цифровой*. Состоит в создании *противником* и/или *нарушителем*, не владеющим *ключом секретным*, пары (сообщение, подпись), которая будет принята как корректная алгоритмом проверки *подписи цифровой*. В зависимости от того, для каких сообщений *противник* и/или *нарушитель* может подделывать подписи, различают подделку *подписи цифровой* универсальную, подделку *подписи цифровой* экзистенциальную и подделку *подписи цифровой* выборочную.

Подмена [substitution] — атака на *криптосистему*, состоящая в перехвате *противником* и/или *нарушителем* сообщения и замене его другим сообщением. При этом выбор последнего может зависеть от перехваченного сообщения.

Подпись цифровая [digital signature, син.: цифровая подпись] — представляет собой цифровую строку, зависящую от подписываемого сообщения или документа и от *секретного ключа* автора. К *подписи цифровой* предъявляются следующие требования: она должна быть легко проверяемой без получения доступа к *секретному ключу,* осуществлять *аутентификацию источника данных,* устанавливать *целостность* сообщения или электронного документа и обеспечивать невозможность отказа от факта подписи конкретного сообщения или документа.

Подпись цифровая групповая [group digital signature] — *цифровая подпись,* в которой правом вычисления значения подписи обладают только члены определенной группы участников, каждый из которых обладает своим *ключом секретным.* Проверка осуществляется с помощью единственного *ключа открытого*.

Подпись цифровая многократная [multiple digital signature] — *цифровая подпись* не являющаяся одноразовой подписью.

Подпись цифровая, не допускающая отказа [undeniable digital signature] — *подпись цифровая*, предусматривающая участие подписавшего в процедуре проверки ее подлинности. Факт подписания того или иного сообщения остается конфиденциальным и может быть установлен только с согласия подписавшего. С помощью специального *протокола* подписавший может доказать с нулевым разглашением, что подпись корректна, либо, напротив, некорректна.

Подпись цифровая одноразовая [one-time digital signature] — *подпись цифровая*, в которой после проведения процедуры проверки правильности необходимо осуществлять смену *ключей.*

Подпись цифровая с восстановлением сообщения [digital signature with message recovery] — разновидность *подписи цифровой*, в которой передается только *подпись цифровая*, а получатель извлекает из нее сообщение при помощи алгоритма проверки *подписи цифровой*.

Подпись цифровая слепая [blind digital signature] — *подпись цифровая,* применяемая к специально сформированному сообщению, из которого без знания *ключа секретного* нельзя получить никакой *информации* о том сообщении, которое будет извлечено из него вместе с корректной подписью получателем. Используется в системах электронных платежей как средство обеспечения неотслеживаемости.

Подпись электронная [electronic signature] — реквизит электронного документа, призванный обеспечивать *идентификацию пользователя*, подтверждение *целостности* подписываемого документа, а также невозможности отказа от факта подписи. Применяются различные технологии, использующие биометрические характеристики, *подписи цифровые*, ключи электронные, пластиковые карты и др.

Подпись электронная цифровая (ЭЦП) [electronic digital signature] — электронный аналог *подписи цифровой,* используемый в системах электронного документооборота для придания электронному документу юридической силы, равной бумажному документу, подписанного собственноручной подписью правомочного лица и скрепленного печатью. ЭЦП является частным случаем *подписи электронной*.

Поле конечное [finite field, Galois field, син.: поле Галуа] — поле, состоящее из конечного числа элементов. Это число есть натуральная степень n простого числа p. К. п. обозначается через F_{p^n} или $GF(p^n)$. Для любого p^n имеется лишь одно с точностью до изоморфизма такое поле.

Политика ИОК [policy certification authority(PCA)] — набор положений, определяющих права и обязанности субъектов ИОК, а также порядок изготовления и использования *сертификатов открытых ключей*.

Полнота (протокола) [completeness property] — свойство *протокола криптографического,* означающее, что при его строгом выполнении участниками *протокол* решает ту задачу, для которой он создан.

Пользователь [user] — лицо, осуществляющее предписанные политикой безопасности действия при взаимодействии с информационной системой.

Пользователь сертификата [relying party, син.: доверяющая сторона] — субъект, полагающийся на достоверность сведений, содержащих-

ся в *сертификат*е *открытого ключа*, и/или ЭЦП, подтвержденную с использованием данного сертификата.

Последовательность [sequence] — математический термин, обозначающий функцию, заданную на множестве натуральных чисел.

Последовательность ключевая [key stream] — в *алгоритмах шифрования поточных — последовательность управляющая*, однозначно определяющая в каждом такте выбор функции зашифрования для зашифрования очередного символа *текста открытого*. Иногда термин п. к. используется в качестве синонима *гаммы* в шифре гаммирования.

Последовательность линейная конгруэнтная [linear congruent sequence] — *последовательность* рекуррентная *u(l), u(2), ...* над кольцом целых чисел с законом рекурсии *u(i + 1) = (a u (i) + b) mod N, i = 1,2,...*

Последовательность линейная рекуррентная [linear recurrent sequence] — *последовательность* рекуррентная *u(1), u(2),...* над конечным полем F_q с линейным законом рекурсии $u(i+m)=\sum_{n=0}^{m-1} a_n u(i+n)$, где $m>0$ — порядок, $\{a_1,...,a_{m-1}\}$ — коэффициенты; $x^m-\sum_{n=0}^{m-1} a_n x^n$ — характеристический многочлен п. л. р.

Последовательность линейная рекуррентная максимального периода [maximal period linear recurrent sequence] — *последовательность линейная рекуррентная* порядка m над полем F_q, у которой период — максимально возможный, равен q^m*-1* и достигается в случае, когда многочлен характеристический является *многочленом примитивным*.

Последовательность псевдослучайная [pseudo-random sequence] — *последовательность*, порожденная детерминированным устройством или программой, вероятностно-статистические свойства которой «близки» (по определенным критериям) к свойствам *последовательности случайной равномерно распределенной* (чисто случайной).

Последовательность случайная [random sequence, син.: случайный процесс с дискретным временем, временной ряд] — *последовательность* случайных величин $x_t \in A$, $t=0,1,\ldots$, заданных на одном и том же

вероятностном пространстве (Ω, F, P). Если A — дискретное множество, то имеем дискретный временной ряд. П. с. полностью задается согласованной системой всевозможных конечномерных распределений вероятностей элементов этой *последовательности*.

Последовательность случайная равномерно распределенная [uniformly distributed random sequence, син.: чисто случайная, последовательность чисто случайная, последовательность случайная равновероятная] — *последовательность* независимых в совокупности случайных величин, имеющих равномерное распределение на заданном конечном *алфавите* $A = \{0,1,\ldots N-1\}$, мощности $2 \le N < +\infty$, характеризуемая следующими двумя свойствами: 1) все возможные значения x_t равновероятны: $\mathrm{P}\ x_t = 0\ = \ldots = \mathrm{P}\ x_t = N-1\ = 1/N$; 2) случайные величины $x_{t_1}, \ldots, x_{t_n}$ независимы в совокупности для любых n, $1 \le t_1 < t_2 < \ldots < t_n$.

Последовательность управляющая [control sequence] — *последовательность псевдослучайная* или *последовательность чисто случайная*, используемая при реализации *алгоритма криптографического*. Частными случаями являются *гамма* шифра и *последовательность ключевая*.

Преобразование, не распространяющее искажений [transform free of error propagation] — см. *отображение, не распространяющее искажений*.

Преобразование перемешивания [mixing transform] — преобразование, с помощью которого стремятся обеспечить свойство перемешивания [mixing property], т.е. существенно усложнить взаимосвязи статистических и аналитических характеристик *текста зашифрованного* по сравнению с подобными взаимосвязями *текста открытого*. Термин «перемешивание» перенесен в *криптографию* К. Шенноном из теории информации.

Преобразование рассеивания [diffusion transform] — преобразование, для которого каждый знак *текста открытого* влияет на большое число знаков *текста шифрованного*. Термин введён К. Шенноном.

Примитив криптографический [cryptographic primitive] — функция (семейство функций), которая используется как составной элемент при построении *криптосистем (протоколов криптографических)* и обладает

требуемыми свойствами. Примеры п. к.: *функция односторонняя, хэш-функция, генератор последовательностей псевдослучайных,* семейство функций псевдослучайных. Иногда п. к. называют такие объекты, как *подпись цифровая,* сертификат *ключа* и т. п., если они используются при построении *протокола криптографического*.

Программные средства [software means] — см. *средства программные*.

Программно-аппаратные средства [software-hardware means] — см. *средства аппаратно-программные*.

Противник [adversary, син.: нарушитель] — внешний по отношению к участникам *протокола криптографического* (*системы криптографической*) субъект (или коалиция субъектов), наблюдающий за передаваемыми сообщениями, и, возможно, вмешивающийся в работу участников, путем перехвата, искажения (модификации), вставки (создания новых), повтора и перенаправления сообщений, блокирования передачи и т. п. с целью нарушения одной или нескольких функций-сервисов безопасности. Может образовывать коалицию с *нарушителем*.

Противник активный [active adversary, син.: нарушитель] — *противник*, который вмешивается в ход выполнения *протокола криптографического* или работу *системы криптографической*. Как правило, полный анализ всех результатов однократного выполнения *протокола криптографического* позволяет обнаружить присутствие противника активного.

Противник пассивный [passive adversary, eavesdropper, син.: наршитель] — *противник*, который может получать некоторую *информацию* о выполнении *протокола криптографического* или работы *системы криптографической*, но не вмешивается в их работу. В случае *протоколов* полный анализ результатов неоднократного их выполнения не позволяет обнаружить присутствие п. п.

Протокол аутентификации [authentication protocol] — *протокол криптографический* установления подлинности взаимодействующих объектов (*пользователей*, программ, технических средств). П. а., как правило, основан на известной обеим сторонам *информации* (*пароли,* личные идентификационные номера, *ключи секретные* или *ключи от-*

крытые) и реализуется с использованием техники «запрос-ответ» или *доказательства знания.* См. также *аутентификация.*

Протокол аутентификации двусторонней (взаимной) [mutual authentication protocol] — *протокол аутентификации* сторон, при выполнении которого каждая из сторон проверяет, что взаимодействующая с ней сторона — именно та, за которую себя выдает. См. также *аутентификация взаимная.*

Протокол аутентификации «запрос-ответ» [challenge-handshake authentication protocol] — *протокол аутентификации односторонней*, при выполнении которого проверяющая сторона направляет запрос доказывающей стороне, а доказывающая сторона направляет ответ на запрос проверяющей стороне.

Протокол аутентификации односторонней [one-way authentication protocol] — *протокол аутентификации,* при выполнении которого одна из сторон (проверяющая) проверяет, что взаимодействующая с ней сторона (доказывающая) — именно та, за которую себя выдает. См. также *аутентификация односторонняя.*

Протокол аутентификации с участием третьей доверенной стороны [trusted third party authentication protocol] — *протокол аутентификации,* при выполнении которого участники взаимодействуют с доверенной стороной. При этом третью сторону называют сервером аутентификации или *арбитром*.

Протокол аутентификации с нулевым разглашением [zero-knowledge protocol] — *протокол аутентификации односторонней*, при выполнении которого проверяющая сторона не получает никакой *информации* о доказываемом утверждении, кроме факта его истинности.

Протокол выработки общего ключа [public key distribution, син.: протокол открытого распределения ключей] — *протокол управления ключами,* в котором *пользователи* вырабатывают (общий) *ключ секретный* путем обмена сообщениями по открытому *каналу связи. Протокол* должен исключать возможность получения *нарушителем* и/или *противником информации* о вырабатываемом *ключе секретном* до завершения действий, предусмотренных *протоколом*. К п. в. о. к. относят также *протокол* Диффи—Хеллмана.

Протокол генерации ключей [key generation protocol] — *протокол управления ключами*, определяющий порядок создания *ключей*.

Протокол голосования [election scheme, voting scheme, voting protocol] — *протокол криптографический,* позволяющий проводить процедуру голосования, в которой избирательные бюллетени существуют только в электронной форме.

Протокол криптографический [cryptographic protocol, син.: криптопротокол] — протокол, предназначенный для выполнения функций *системы криптографической,* в процессе выполнения которого участники используют *алгоритмы криптографические.* Например, к п. к. относят: *протокол аутентификации, протокол управления ключами.*

Протокол проверки статуса сертификата онлайновый [online certificate status protocol, OCSP] — *протокол криптографический*, дающий возможность проверить on-line статус данного неквалифицированного сертификата.

Протокол (схема) разделения секрета [secret sharing scheme] — *протокол управления ключами*, основанный на *схеме разделения секрета.*

Протокол распределения ключей [key distribution protocol] — *протокол криптографический* получения *пользователями ключей,* необходимых для функционирования *системы криптографической.* Различают следующие типы п. р. к.: *протоколы* передачи (уже сгенерированных) *ключей*; *протоколы* совместной выработки общего *ключа* (*распределение ключей* открытое*); схемы распределения ключей предварительного.*

Протокол распределения ключей телеконференции [teleconference key distribution protocol] — *протокол распределния ключей*, в котором участники объединены в группы, и различные группы должны иметь различные *ключи*.

Протокол с разглашением нулевым [zero-knowledge protocol] — *протокол аутентификации односторонней*, при выполнении которого проверяющая сторона не получает никакой *информации* о доказываемом утверждении, кроме факта его истинности. См. также *доказательство с разглашением нулевым.*

Протокол смены ключа [key update protocol] — *протокол управления ключами*, определяющий порядок смены, контроля *целостности* и обеспечения *конфиденциальности ключей секретных алгоритма криптографического*. Для *ключей открытых алгоритма криптографического* должен быть обеспечен контроль *целостности*.

Протокол уничтожения ключа [key destruction protocol] — *протокол управления ключами*, определяющий порядок уничтожения *ключа секретного алгоритма криптографического*, обеспечивающий невозможность полного или частичного восстановления *ключа*.

Протокол управления ключами [key management protocol] — *протокол криптографический*, определяющий в соответствии с установленной политикой безопасности порядок генерации, распределения, использования, смены, хранения, архивирования, восстановления и уничтожения *ключей*, а также замены скомпрометированных *ключей*.

Протокол хранения ключа [key escrow system] — *протокол управления ключами*, определяющий порядок хранения, контроля *целостности* и обеспечения *конфиденциальности ключа секретного алгоритма криптографического*. Для *ключа открытого алгоритма криптографического* должен быть обеспечен контроль *целостности*.

Псевдоколлизия [pseudocollision] — событие, при котором значения *хэш-функции*, зависящей от *ключа*, совпадают для различных значений сообщения и *ключа*.

Пункт доверия [point of trust] — издатель первого сертификата, а также *центр удостоверяющий*, признаваемый пунктом доверия в архитектуре ИОК.

Р

Разглашение нулевое [zero-knowledge property] — свойство протокола *доказательства знания,* обеспечивающее такое его выполнение, что никакая *информация* о доказываемом утверждении, кроме факта его истинности, не может быть получена нечестным проверяющим из переданных сообщений за время полиномиально зависящее от суммарной длины этих

сообщений.

Разделение секрета линейное [linear secret sharing] — разделение секрета, при котором вспомогательным секретом считается вектор *s* из *n*-мерного векторного пространства F_q^n над конечным полем. Секретом s_0 и его частичными секретами s_i считаются образы *s* при линейных отображениях $s_i = f_i(s),\ i = 0,1,...,l$ на некоторые подпространства $L_0, L_1, ..., L_l \subset F_q^n$. Если эти подпространства удовлетворяют определенным условиям, то путем р.с.л. можно получить совершенную реализацию любой структуры доступа.

Разделение секрета модулярное [modular secret sharing] — разделение секрета, базирующееся на модулярной арифметике в кольце целых чисел. Секрет отождествляется с целым числом, а *частичный секрет* участника является остатком от деления его на *ключ открытый* (модуль) участника. Для восстановления секрета привлекается китайская теорема об остатках. Модулярный подход к разделению секрета обобщается на случай колец многочленов от одной и нескольких переменных над полями Галуа.

Распределение ключей [key distribution] — установленный порядок распространения *ключей*.

Расстояние единственности [unicity distance] — минимальное количество выходных данных *системы криптографической* (например, начального отрезка *текста шифрованного*), с заданной вероятностью достаточное для однозначного определения неизвестного параметра (например, *ключа секретного*) этой системы.

Расстояние Хэмминга [Hamming distance] — число позиций, в которых различаются два вектора одинаковой длины.

Расширение ключа [key expansion] — преобразование *ключа секретного*, увеличивающее его длину. Расширенный *ключ* применяется затем для *зашифрования*. Процедура р. к. имеет своей целью усложнить зависимость *текста шифрованного* от *ключа*.

Расшифрование [decryption, deciphering, син.: функция расшифрования] — математическое преобразование, обратное к *зашифрованию* и

реализуемое при известном *ключе расшифрования*.

Регистр сдвига с динамическим изменением линейной обратной связи [dynamic linear feedback shift register] — *регистр сдвига с обратной связью* длины n, у которого функция обратной связи f может изменяться от такта к такту на фиксированном множестве функций.

Регистр сдвига с линейной обратной связью [linear feedback shift register (LFSR), син.: регистр сдвига линейный] — *регистр сдвига с обратной связью* длины n, у которого функция обратной связи f линейна.

Регистр сдвига с нелинейной обратной связью [nonlinear feedback shift register] — *регистр сдвига с обратной связью* длины n, у которого функция обратной связи f нелинейная.

Регистр сдвига с обратной связью [feedback shift register] — регистром сдвига длины n над множеством X с функцией обратной связи f называют конечный автономный автомат с множеством состояний X^n. Находясь в состоянии $(x_1,\ldots,x_n)$, р. с. вырабатывает выходной символ x_1 и переходит в состояние $(x_2,\ldots,x_n,f(x_1,\ldots,x_n))$. Рассматриваются различные обобщения понятия р. с. с о. с.: неавтономный, обобщенный, регистр сдвига с иными функциями выхода и др. Р. с. с о. с. как техническое устройство используется при реализации различных компонентов *систем криптографических,* например, генераторов фильтрующих, генераторов комбинирующих.

Регистр сдвига с обратной связью и переносом [feedback with carry shift register] — *регистр сдвига с обратной связью* длины n, у которого функция обратной связи f зависит от текущего состояния регистра и бита переноса определяемого предыдущими состояниями регистра.

Регистр сдвига со многими линейными обратными связями [multiple linear feedback shift register] — *регистр сдвига с обратной связью* длины n, у которого в каждый момент времени используются k $(1<k\leq n)$ функций обратной связи, линейных над конечным полем (кольцом).

Режим выработки имитовставки (кода аутентификации) [message authentication code mode] — см. *алгоритм выработки кода аутентификации.*

Режим шифрования блочного алгоритма [block cipher modes of operation] — способ получения *алгоритма шифрования блочого* конкретного текста, исходя из базового *блочного алгоритма* зашифрования. Основными р. ш. являются: простая замена или электронная кодовая книга (ECB), сцепление блоков шифртекста (CBC), обратная связь по шифртексту (CFB), обратная связь по выходу (OFB).

С

Связь правительственная [government channel, government link, син.: правительственная (телефонная и документальная) связь] — вид *специальной связи* для передачи речевой и документальной *информации*, функционирующий для обеспечения органов государственного управления.

Связь специальная [special communication] — вид связи (электросвязи), предназначенный для защищенной передачи *информации* с применением криптографических, технических и иных средств и методов защиты *информации*, включая правительственную, оперативную и другие виды связи, используемые в том числе для обеспечения безопасности оперативно-розыскной, разведывательной и контрразведывательной деятельности.

Связь шифрованная (шифросвязь) [secret communication] — вид *специальной связи*, организуемой с помощью ручных шифров или *аппаратуры шифрования* в целях обеспечения сохранения государственной и служебной тайны при передаче сообщений по техническим средствам связи.

Секрет пользователя частичный [share, secret share, син.: доля секрета] — ключевая *информация*, получаемая отдельным участником *схемы разделения секрета,* позволяющая ему вместе с другими участниками разрешенного подмножества восстанавливать значение секрета.

Сертификат открытого ключа [public key certificate, ISO/IEC 11770-3] — электронный документ, созданный и подписанный удостоверяющим центром и содержащий информацию, подтверждающую принадлежность *открытого ключа* конкретному физическому или юридическому лицу.

Сертификат открытого ключа отозванный [revocation certificate] — *сертификат открытого ключа*, включенный *центром удостоверяющим* в *список отозванных сертификатов*.

Сертификат самоподписанный [self-signed certificate, син.: самоизданный сертификат, самозаверенный сертификат] — специальный тип сертификата, изданный и подписанный *удостоверяющим центром* ИОК в соответствии с политикой безопасности ИОК. См. *корневой удостоверяющий центр*, *корпоративная ИОК*.

Сертификационные испытания средств криптографической защиты информации [cryptographic module certification tests] — испытания *средств криптографической защиты информации* в аккредитованных испытательных лабораториях с целью проверки выполнения требований технических нормативных правовых актов по безопасности *информации*. Дополнительно могут проводиться сертификационные испытания аппаратно-программных и аппаратных *средств криптографической защиты информации* на соответствие техническим нормативным правовым актам по электромагнитной безопасности и/или электромагнитной совместимости.

Сертификация ключей открытых [public-key certification] — процесс формирования данных, которые позволяют в дальнейшем осуществлять аутентификацию и контроль целостности *открытого ключа*, а также проверку того, что данный ключ принадлежит участнику информационного обмена, за которого он себя выдает.

Сеть засекреченной связи [encryption telecommunications, син.: сеть шифрованной связи] — см. *сеть шифрованной связи*.

Сеть шифрованной связи [encryption telecommunications, син.: сеть засекреченной связи] — совокупность корреспондентов, имеющих однотипную *аппаратуру шифровальную* (один и тот же код) и одинаковую *документацию ключевую*.

Синхропосылка [synchrosignal] — комбинация знаков, передаваемая по *каналу связи* и предназначенная для вхождения в связь *аппаратуры шифрования* или для синхронизации аппаратуры. См. также *вектор инициализации*.

Система ключевая [key system, key management] — система, состоящая из *ключевого множества*, *системы установки ключей* и *системы управления ключами*.

Система криптографическая [cryptographic system (cryptosystem), син.: криптосистема, криптографическая система защиты информации] — система обеспечения безопасности *информации* в части *конфиденциальности, целостности, аутентификации,* невозможности отказа и неотслеживаемости с использованием *средств криптографической защиты информации.* В качестве подсистем может включать *систему шифрования,* систему идентификации, систему имитозащиты, систему электронной цифровой подписи и др., а также *систему ключевую,* обеспечивающую функционирование остальных систем. Главный критерий при построении с. к. — обеспечение *стойкости криптографической*.

Система управления ключами [key management system] — подсистема *системы ключевой*, определяющая порядок регистрации *ключей*, их использования, смены, хранения и архивирования, резервного копирования и восстановления, замены или изъятия из обращения скомпрометированных, а также уничтожения старых *ключей*. Целью управления *ключами* является нейтрализация таких угроз, как *компрометация* и несанкционированное использование *ключей*, например, использование *ключа*, срок действия которого истек.

Система установки ключей [key establishment system] — подсистема *системы ключевой*, определяющая алгоритмы и процедуры генерации, распределения, передачи и проверки *ключей*.

Система шифрования [cryptosystem, cipher, син.: шифрсистема] — *система криптографическая*, предназначенная для защиты *информации* от лиц, не имеющих права доступа к ней. Защита обеспечивается путем *зашифрования информации*. Математическая модель с. ш. включает способ кодирования исходной и выходной *информации*, *шифр* и *систему ключевую*.

Система шифрованной связи [secure communication system, син. система засекреченной связи] — система связи, в которой конфиденциальность передаваемой *информации* обеспечивается комплексом организационно-технических мер с применением *аппаратуры шифровальной*.

Система шифрованной связи государственная [national public security communication system] — *система шифрованной связи*, предназначенная для передачи и защиты документальной и иной *информации*, отнесенной к государственным секретам, с использованием сетей электросвязи.

Сложность линейная [linear complexity] — наименьшая длина *регистра сдвига линейного,* порождающего периодическую *последовательность*.

Служба шифровальная [encryption department, син.: шифровальная служба] — система специальных подразделений (органов), обеспечивающих защиту и (или) *имитозащиту информации* при ее передаче по техническим средствам связи или другим каналам вне контролируемой зоны.

Смена ключей [key update] — порядок действий, определяющий замену *ключа* с истекшим сроком действия на другой *ключ*.

Совершенная схема разделения секрета [perfect secret sharing scheme] — *схема разделения секрета*, в которой *частичные секреты* любого неразрешенного множества участников не позволяет получить никакой *информации* о значении секрета, кроме априорной.

Согласование ключей [key agreement] — последовательность действий, направленная на получение одинаковых *ключей* у двух абонентов сети с использованием криптографических *протоколов* для последующего *шифрования* данных.

Сообщение зашифрованное [ciphertext, син.: сообщение шифрованное, шифртекст] — сообщение, полученное в результате *зашифрования сообщения открытого*.

Сообщение открытое [plaintext, cleartext, син.: текст открытый] — см. *текст открытый.*

Список отозванных сертификатов [certificate revocation list, CRL] — *электронный документ*, созданный и подписанный *удостоверяющим центром* и содержащий *информацию* о *сертификатах открытых клю-*

чей, выпущенных данным *удостоверяющим центром*, действие которых прекращено или приостановлено до истечения срока действия *открытых ключей*.

Средства аппаратные [hardware means] — все или часть физических компонентов системы обработки *информации*.

Средства аппаратно-программные [software-hardware means, син.: средства программно-аппаратные] — *средства аппаратные* с размещенными программами и данными. Программы должны быть размещены таким образом, чтобы их несанкционированное изменение было невозможно в ходе исполнения. Программы и данные, размещенные на ПЗУ с электронным программированием, допускающим стирание (EEPROM), рассматриваются как программное обеспечение.

Средства аутентификации [message authentication tools] — средства, предназначенные для опознавания сторон (субъектов и (или) объектов) в процессе информационного взаимодействия.

Средства защиты аппаратные [security hardware, аппаратные средства защиты] — механические, электромеханические, электронные, оптические, лазерные, радио, радиотехнические, радиолокационные и другие устройства, системы и сооружения, предназначенные для защиты *информации* от несанкционированного доступа, копирования, кражи или модификации.

Средства защиты государственных секретов [State secrets security services] — *средства защиты информации* используемые для защиты *информации,* содержащей государственные секреты.

Средства защиты информации [security mechanisms] — *средства технической защиты информации*, *средства криптографические* и иные средства, предназначенные для защиты *информации*, средств, в которых они реализованы, а также средства контроля эффективности защиты *информации*.

Средства имитозащиты [integrity protection tools] — аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования *информации* и предназначенные для защиты от навязывания ложной *информации*.

С. и. относятся к *средствам криптографической защиты информации*.

Средства криптографические [cryptographic tools, cryptographic mechanisms] — в широком смысле — средства обеспечения безопасности *информации*, использующие *функции криптографические*; в узком смысле — средства, реализованные в виде документов, механических, электромеханических, электронных, технических устройств или программ, предназначенные для выполнения функций *системы криптографической*.

Средства криптографические аппаратные [cryptographic hardware (device, facility)] — *средства криптографические*, реализованные в виде специальных технических устройств. Реализуют одну или несколько *функций криптографических* или их частей.

Средства криптографические встраиваемые [build-in cryptographic mechanisms] — *средства криптографические*, внешние по отношению к операционной системе средств вычислительной техники, но зависящие от нее. К ним, например, относятся различные интерфейсы прикладного программирования и средства встраиваемые на сетевом уровне.

Средства криптографические выше прикладного уровня [above the application layer cryptographic mechanisms] — *средства криптографические*, реализованные таким образом, что все данные заранее преобразуются так, чтобы они могли быть переданы непосредственно с помощью существующего *протокола* прикладного уровня, и чтобы при этом были реализованы необходимые службы и обеспечивался необходимый *уровень безопасности*.

Средства криптографические защиты государственных секретов (СКЗГС) [state secrets security services, син.: криптографические средства защиты государственных секретов] — *средства криптографической защиты информации*, предназначенные для защиты *информации*, содержащей государственные секреты. СКЗГС относятся как к *средствам криптографической защиты информации*, так и к *средствам защиты государственных секретов*. СКЗГС отличаются от *средств криптографической защиты информации* повышенными требованиями к ним и являются составной частью *средств защиты государственных секретов*.

Средства криптографические защиты информации (СКЗИ) [cryptographic information protection facility, син.: средства криптографической защиты информации] — технические, программные, программно-технические *средства защиты информации*, реализующие *алгоритмы криптографические* и *протоколы*, а также функции управления криптографическими *ключами*.

К средствам криптографической защиты информации относятся:

- *средства шифрования*, включая средства изготовления ключевых документов (независимо от вида носителя ключевой *информации*) и управления криптографическими *ключами*;
- *средства иммитозащиты*;
- *средства электронной цифровой подписи*;
- *средства* идентификации и аутентификации.

СКЗИ по назначению относятся к *средствам защиты информации*, по выполняемым функциям — к *средствам криптографическим*. Функции защиты от несанкционированного доступа могут осуществлять *средства шифрования*.

Средства криптографические наложенные [additional cryptographic mechanisms] — *средства криптографические*, не связанные с функционированием операционной системы средств вычислительной техники.

Средства криптографические прикладного уровня [application layer cryptographic mechanisms] — *средства криптографические*, реализованные таким образом, что модули, выполняющие *функции криптографические*, расположены только на прикладном уровне и не требуют никаких модификаций для программных модулей и интерфейсов для более низких уровней. Это означает, что для обеспечения функций безопасности должны быть модифицированы как прикладные *протоколы*, так и сами прикладные программы, использующие эти *протоколы*.

Средства криптографические программные [software cryptographic mechanism] —*средства программные*, реализующие одну или несколько криптографических функций-сервисов безопасности. Различают с. к. п. с выполнением в контексте *пользователя* и на уровне ядра или системном уровне операционной системы средств вычислительной техники. С. к. п. с выполнением в контексте *пользователя*, как правило, ориентированы на выполнение ограниченного множества *функций криптографических* и решают какую-либо одну конкретную задачу. Могут быть реализованы как в виде законченного программного продукта, интеграция которого

заключается в обычной инсталляции данного продукта, так и в виде программных модулей, установка которых может требовать дополнительных процедур встраивания их в программное обеспечение. С. к. п. с выполнением на уровне ядра или системном уровне ОС реализуются в виде системных функций, выполняемых на уровне ядра, либо на системном уровне (драйверы, динамические библиотеки). Для унификации реализации и использования *функций криптографических* различными приложениями в этом случае разрабатывается специальный крипто API.

Средства криптографические сетевого уровня [network layer cryptographic mechanism] — *средства криптографические*, реализованные таким образом, что модули, выполняющие *функции криптографические*, расположены только на сетевом уровне без каких бы то ни было модификаций для программных модулей и интерфейсов для уровня канала передачи данных и прикладного уровня.

Средства криптографические транспортного уровня [transport layer cryptographic mechanism] — *средства криптографические*, реализованные таким образом, что модули, выполняющие *функции криптографические*, расположены на транспортном уровне, который осуществляет контроль доставки *информации* и контроль ее *целостности*. Такая реализация имеет целью усиление безопасности сетевого программного интерфейса с помощью введения дополнительных возможностей, а также обеспечения возможности прикладным программам избирательно использовать эти дополнительные возможности.

Средства криптографические физического и канального уровня [physical and data layer cryptographic mechanism] — *средства криптографические*, осуществляющие *шифрование* трафика (соединения) на физическом или канальном уровне, исполненные в виде скремблеров, шифрующих модемов, специализированных канальных адаптеров и т. п.

Средства криптографические штатные [cryptographic services] — *средства криптографические*, заложенные в функциональные возможности операционных систем средств вычислительной техники.

Средства программные [software means син.: программные средства, программное обеспечение] — все или часть программ, процедур, правил и относящаяся к ним документация системы обработки *информации*.

Средства технической защиты информации [information technical protection facilities] — технические средства, предназначенные для предотвращения утечки *информации* по одному или нескольким техническим каналам.

Средства шифрования [encryption means, син.: шифровальные средства] — *криптографические средства*, предназначенные для обеспечения *конфиденциальности информации* путем *шифрования* при ее обработке, хранении и передаче. С. ш. относятся к *средствам криптографической защиты информации*. С. ш. обеспечивают защиту от несанкционированного доступа к *информации* путем использования функции *зашифрования*.

Средства электронной цифровой подписи [electronic digital signature mechanism] — средства, реализующие одну или несколько из следующих *криптографических функций*: выработка *электронной цифровой подписи*, проверка *электронной цифровой подписи*, выработка *личного ключа* и *открытого ключа электронной цифровой подписи*, генерации параметров системы *электронной цифровой подписи*.

Срок действия ключа [key life cycle] — промежуток времени, в течение которого *ключ* может быть использован доверенными сторонами. Срок действия *ключа* устанавливается для ограничения объёма *информации*, зашифрованной на данном *ключе*, которая может быть использована для *криптоанализа* и для ограничения размера ущерба при его *компрометации*. Необходимо иметь в виду, что термин относится только к сроку действия *ключа*, а не к промежутку времени, в течение которого *ключ* должен оставаться в секрете.

Стандарт подписи электронной цифровой [digital signature standard] — утвержденный техническим нормативным правовым актом алгоритм выработки и проверки *электронной цифровой подписи*.

Стандарт функции хэширования [hash standard] — утвержденный техническим нормативным правовым актом алгоритм вычисления *хэш-функции*.

Стандарт шифрования [encryption standard] — утвержденный техническим нормативным правовым актом *алгоритм шифрования*.

Стеганография [steganography] — направление *криптологии* (в широком смысле), имеющее целью разработку средств защиты (передачи и хранения) *информации*, которые скрывают сам факт ее защиты (передачи и хранения). В частности, для стеганографической передачи *информации* внутри открытого канала создается скрытый канал, не обнаруживаемый нелигитимным абонентом. В настоящее время основными областями применения стеганографии являются: скрытая связь; защита от копирования с помощью цифровых водяных знаков (watermarking); скрытая аннотация и доказательство аутентичности документов (fingerprinting, captioning).

Стойкость доказуемая [provable security] — понятие, определяемое в рамках некоторой математической модели данной криптосистемы. В настоящее время имеются два подхода к определению этого понятия: теоретико-информационный и теоретико-сложностный.

Стойкость гарантированная [guaranteed security] — стойкость *шифра*, который при соблюдении всех правил его пользования не может быть раскрыт аналитическими методами в течение заданного промежутка времени.

Стойкость криптографическая [cryptographic security, син.: криптостойкость] — свойство *криптосистемы* (*криптопротокола*), характеризующее её (его) способность противостоять атакам *противника* и/или *нарушителя*, как правило, имеющим целью получить *ключ секретный* или *текст открытый*. Развиваются два основных подхода к определению и оценке стойкости — *стойкость теоретическая (доказуемая)* и *стойкость практическая*.

Стойкость (криптосистемы) практическая [practical security (of the cryptosystem)] — вычислительная сложность алгоритма, реализующего наилучшую в определенном смысле *атаку на криптосистему*. Чаще всего под с. п. понимают временную сложность выполнения успешной *атаки на криптосистему* наиболее быстрым из известных алгоритмов при реальных предположениях о свойствах *криптосистемы* и ее применении, а также о вычислительных машинах, на которых она будет реализовываться. Дополнительными характеристиками атаки также являются: вероятность успеха атаки, необходимый объем памяти, вычислительная сложность подготовительной стадии, необходимый объем памяти для подготовительной стадии. Такой подход, с учетом перспектив увеличе-

ния производительности вычислительных машин, позволяет оценить время, в течение которого данная *криптосистема* будет обеспечивать защищенность *информации*.

Стойкость примитива криптографического [security of a cryptographic primitive] — соответствие свойств *примитива криптографического* его предназначению. Например, стойкость *функции односторонней* предполагает отсутствие эффективных (полиномиальных) алгоритмов ее инвертирования, стойкость *хэш-функции криптографической* — отсутствие эффективных методов построения коллизий.

Стойкость (шифрсистемы) совершенная [perfect secrecy] — свойство *системы шифрования*, заключающееся в том, что *текст шифрованный* не содержит *информации* о *ключе* и *тексте открытом*, кроме, возможно, его длины. Например, таким свойством обладает шифрсистема гаммирования, если применяемая *гамма* является реализацией *последовательности случайной равномерно распредленной (чисто случайной)*.

Стойкость (криптосистемы) теоретическая [theoretical security, син.: доказуемая] — *стойкость криптографическая*, определяемая в рамках некоторой математической модели. Основные подходы к определению с. т. в настоящее время — *стойкость теоретико-информационная* и *стойкость теоретико-сложностная*. Рассмотрение с. т. в рамках абстрактных математических моделей позволяет говорить о *стойкости доказуемой*.

Стойкость теоретико-информационная (шенноновская) [information-theoretic (Shannon) security] — вид *стойкости теоретической*, определяемый с точки зрения математической теории *информации*. С. т.-и. *криптосистемы* обычно характеризуется *количеством информации* (в смысле К.Шеннона) относительно неизвестного *противнику* и/или *нарушителю ключа секретного* или *текста открытого*, содержащимся в перехваченном *тексте шифрованном* или других доступных данных и вычисленным в рамках той или иной вероятностной модели. Говорят также, что с. т.-и. *криптосистемы* характеризует ее способность противостоять атакам со стороны *противника* и/или *нарушителя*, располагающего неограниченными вычислительными ресурсами.

Стойкость теоретико-сложностная [complexity-based security] — вид *стойкости теоретической*, определяемый с точки зрения математиче-

ской теории сложности алгоритмов. С. т.-с. *криптосистемы* означает оценку сложности *атак* со стороны *противника* и/или *нарушителя*, располагающего ограниченными вычислительными ресурсами, на неизвестные параметры *криптосистемы* (например, *ключ секретный* или *текст открытый*). Как правило, с. т.-с. основывается на предположении о вычислительной сложности математической задачи, на основе которого доказывается с. т.-с.

Структура доступа [access structure] — разбиение семейства всех подмножеств конечного множества участников на два подсемейства. Множества из первого семейства называются разрешенными (правомочными), а множества из второго — неразрешенными. Обычно еще предполагают выполненным условие монотонности — при добавлении участника к разрешенному подмножеству оно остается разрешенным.

Структура доступа пороговая [threshold access structure, (k,t) - threshold access structure] — *структура доступа* на множестве, состоящем из *t* участников при условии, что разрешенными являются подмножества стоящие из *k* и более участников. Число *k* называется порогом.

Схема разделения секрета [secret sharing scheme] — состоит из алгоритмов разделения и восстановления секрета и *структуры доступа*. Алгоритм разделения секрета преобразует секрет *s* в набор *частичных секретов* $s_1, s_2 \ldots s_t$. Частичный секрет s_i передается *i*-му участнику. Алгоритм восстановления секрета однозначно восстанавливает секрет *s*, если на вход поданы частичные секреты разрешенного подмножества (правомочной коалиции) участников, а частичные секреты неразрешенного подмножества не позволяют получить секрет *s*.

Схема разделения секрета идеальная [ideal secret sharing scheme] — *схема разделения секрета,* в которой число битов, содержащихся в каждом *частичном секрете,* равно числу битов, содержащихся в самом секрете. Иногда в это определение добавляют условие совершенности.

Схема разделения секрета пороговая [threshold secret sharing scheme] — *схема разделения секрета* для *структуры доступа пороговой*.

Схема распределения ключей предварительного [preliminary key distribution scheme] — *схема разделения секрета,* применяемая в сети

связи для уменьшения объема хранимой *информации* о *ключах.* Суть с. р. к. п. состоит в том, что предварительно распределяются не *ключи*, а сгенерированные в *центре распределения ключей* секретные данные меньшего объема, по которым каждый *пользователь* самостоятельно вычисляет по оговорённому алгоритму необходимый для связи *ключ*. С. р. к. п. должна быть устойчивой относительно компрометации части *ключей*, в том числе, вследствие обмана или сговора некоторых *пользователей*, и гибкой, то есть быстро восстанавливаться как после частичной *компрометации*, так и после подключения новых *пользователей*.

Схема Фейстеля [Feistel scheme, син.: преобразование Фейстеля] — способ построения цикла (раунда) *шифрования* в *алгоритмах шифрования* итеративных (блочных) на основе *регистра сдвига нелинейного* длины 2 с функцией обратной связи, зависящей от *ключа циклового* (раундового). Схема названа по имени одного из разработчиков и запатентована в США в 1974 г.

Схема Шамира [Shamir's threshold scheme] — *пороговая схема разделения секрета.* Секретом является $s=f(0)$ – свободный член многочлена над конечным полем, а *частичными секретами* – значения того же многочлена $f(x_1),f(x_2),\ldots,f(x_t)$, где $x_1,x_2,\ldots,x_t$ – попарно различные элементы того же поля. Секрет восстанавливается по интерполяционной формуле Лагранжа. Схема Шамира является и совершенной и идеальной.

Схема Шнорра [Schnorr identification protocol] — протокол *идентификации,* основанный на сложности задачи дискретного логарифмирования. Он предусматривает передачу только трех сообщений, а также позволяет проводить предварительные вычисления, что удобно при малых вычислительных ресурсах и сетях с низкой пропускной способностью.

Схема ЭЦП [electronic digital signature scheme, син.: подпись цифровая] — *протокол*, состоящий из *алгоритма выработки ЭЦП* и *алгоритма проверки ЭЦП.*

Т

Тематические исследования [case study] — криптографические, инженерно-криптографические и специальные исследования средств и *систем криптографической защиты информации* с целью проверки выпол-

нения требований по безопасности *информации*.

Текст открытый [plaintext] — данные, подлежащие *зашифрованию* и представленные в некотором конечном *алфавите*.

Текст шифрованный [ciphertext, син.: шифртекст, сообщение зашифрованное] — см. *шифртекст*.

Тест статистический [statistical test, син.: статистический критерий] — правило принятия решений о справедливости одной из гипотез в задаче статистической проверки гипотез. Например, нулевой гипотезы H_0 о том, что параметр p схемы независимых испытаний равен $p = p_0 = 1/2$, против альтернативной гипотезы H_1, состоящей в том, что $|p - p_0| \geq 0.01$. В общем случае т. с. задается критической функцией; нерандомизированный тест может быть задан критической областью, которая определяется статистикой теста и ее распределением вероятностей при нулевой гипотезе.

Техника шифровальная [encryption technology, син.: шифровальная техника, шифртехника] — вид техники, предназначенной для *шифрования*, засекречивания (рассекречивания), кодирования и *имитозащиты информации*, передаваемой по техническим средствам связи, и изготовления *ключевых документов* для обеспечения этих целей.

К т. ш. относятся:

- *аппаратура предварительного шифрования*, включающая *аппаратуру шифровальную* (комплексы), кодировочные машины, сигнально-кодовые и кодирующие устройства;
- засекречивающая аппаратура связи, включающая аппаратуру засекречивания телефонной, телеграфной, факсимильной, телекодовой, телевизионной информации и данных;
- аппаратура изготовления ключевых документов, включающая комплекс приборов, устройств и соответствующих программ, создающих ключи, фиксирующих их на носителе и осуществляющих комплектацию их в ключевые блокноты, а также аппаратура децентрализованного формирования, распределения и передачи ключей по каналам связи;
- групповая засекречивающая аппаратура связи, обеспечивающая засекречивание потоков служебной *информации*;
- аппаратура защиты криптографической, включающая в себя засек-

речивающую аппаратуру защиты телефонной или телекодовой *информации* и аппаратуру *имитозащиты*.

В настоящее время термин в Республике Беларусь выходит из массового употребления. Вместо него в нормативных правовых актах используется термин *шифровальная аппаратура* (см. *аппаратура шифрования*).

У

Угроза [threat] — действия или события, которые могут нарушить свойства *системы криптографической* (*протокола криптографического*), например, *конфиденциальности, целостности, аутентификации, невозможности отказа, неотслеживаемости*.

Узел криптографический [cryptographic node] — составная часть устройства, реализующая подмножество (часть) *алгоритма криптографического* или *протокола криптографического*, или реализующая определенную *функцию алгоритма криптографического* или *протокола криптографического*.

Уничтожение ключей [key destruction] — предписанный руководящими документами порядок уничтожения *документов ключевых* и *ключей* по окончании срока их действия, а также упаковок от *документов ключевых*.

Управление доступом [access control] — определение и ограничение доступа *пользователей*, программ и процессов к данным, программам и устройствам вычислительной системы.

Управление ключами [key management] — администрирование и использование генерации, регистрации, сертификации, отмены регистрации, распространения, установки, хранения, архивирования, аннулирования, создания производственного и уничтожение ключевого материала в соответствии с требованиями безопасности.

Уровень безопасности [security level] — степень защищенности объекта оценки, достигаемая при выполнении заданной совокупности требований.

Уязвимость [vulnerability] — слабое место в безопасности информационной системы, использование которого *противником* и/или *нарушителем* может привести к реализации *угрозы* безопасности.

Ф

Функция криптографическая [cryptographic function, син.: преобразование криптографическое, криптопреобразование] — функция (преобразование), необходимая для построения *системы криптографической*. Примеры ф. к.: функции *зашифрования* и *расшифрования, хэш-функция,* функция вычисления *имитовставки, кода аутентичности сообщения, электронной цифровой подписи,* генерации *ключей*.

Функция хэширования [hash-function, secure hash algorithm, син.: хэш-функция] — отображение $h: A^* \to A^n$ слов произвольной конечной длины в алфавите A в слова заданной длины n. Ф. х. может зависеть от ключа. К ф. х., используемым в *криптографии,* предъявляют требования быть однонаправленными, устойчивыми к *коллизиям* и *псевдоколлизиям.*

Х

Хранение ключей [key escrow] — предписанный руководящими документами порядок хранения и выдачи основных и резервных *ключей* в течение срока их действия.

Хэш-значение [hash-code, hash-result, hash-value, hash, imprint, digital fingerprint, message digest] — значение *хэш-функции* для заданного значения аргумента.

Ц

Целостность [integrity] — отсутствие изменений в передаваемой или хранимой *информации* по сравнению с ее исходной записью. Необходимым условием соблюдения ц. является защищённость сообщения от преднамеренной или случайной несанкционированной модификации или уничтожения.

Центр регистрации [registration authaority] — юридическое лицо, имеющее полномочия подтверждения персональных данных физических лиц и регистрации физических лиц в качестве *пользователей* информационной системы. Дополнительно центр регистрации может выполнять функции по разбору конфликтных ситуаций, связанных с использованием ЭЦП.

Центр удостоверяющий [certification authority] — юридическое лицо, выполняющее функции создания, распространения и хранения *сертификатов открытых ключей* и *списков отозванных сертификатов*.

Центр удостоверяющий корневой [certificate authority] —. главный *центр удостоверяющий* в иерархической структуре центров удостоверяющих, выпускающий самоподписанный *сертификат открытого ключа* для изготовления *сертификатов открытых ключей* подчиненных *центров удостоверяющих*.

Центр эмиссии сертификатов открытых ключей [certificate directory] — техническая и организационная инфраструктура управления *сертификатами открытых ключей*.

Ш

Шифр [cipher, син.: алгоритм шифрования] — см. *алгоритм шифрования***.**

Шифр блочный [block cipher, син.: алгоритм шифрования блочный] — см. *алгоритм шифрования блочный*.

Шифр перестановки [permutation cipher, transposition cipher] — *алгоритм шифрования*, в котором осуществляется разбиение исходного текста на блоки символов одинаковой длины и использование для каждого такого блока некоторой перестановки. *Ключом* такого *шифра* является используемая при *шифровании* перестановка.

Шифр подстановки [substitution cipher] — *алгоритм шифрования*, в котором каждый символ *открытого текста* заменяется на некоторый другой. Сюда же относят и гомофоническое *шифрование*, когда каждая

буква текста шифруется несколькими символами этого или другого *алфавита*. При полиграммном *шифровании* заменяются не буквы текста, а их комбинации.

Шифр поточный [stream encryption algorithm, stream cipher, син.: алгоритм шифрования поточный] — см. *алгоритм шифрования поточный*.

Шифр простой замены [simple substitution cipher, mono-alphabetic substitution cipher] — *алгоритм шифрования*, в котором буквы *текста открытого* заменяются буквами того же или другого *алфавита* в соответствии с некоторой подстановкой (биекцией). Примером является *шифр* Цезаря, когда буквы латинского *алфавита* сдвигаются циклически вправо на три позиции.

Шифр совершенный [perfect cipher] — *шифр*, обладающий свойством: условное распределение на множестве *текстов открытых* при заданном *тексте шифрованном* совпадает с безусловным распределением на множестве *текстов открытых*. Это означает также, что *текст шифрованный* не дает без знания *секретного ключа* никакой *информации* о *тексте открытом*.

Шифратор [encoder, encipher] — *модуль криптографический*, имеющий явно определенный периметр, устанавливающий физические границы модуля, изолированную среду функционирования и формализованные интерфейсы взаимодействия со средой функционирования *шифровальной аппаратуры* и внешней средой, и предназначенный для *зашифрования* и *расшифрования информации*.

Шифровальная аппаратура [cryptographic hardware, enciphering hardware, encryption hardware, син.: аппаратура шифрования, аппаратура шифровальная] — см. *аппаратура шифрования*.

Шифрование [encryption, enciphering] — термин, объединяющий термины *зашифрование* и *расшифрование*.

Шифрование абонентское [end-to-end encryption, син.: шифрование сквозное] — способ *шифрования*, при котором зашифрование данных осуществляется между конечными абонентами (без промежуточного перешифрования на пути от отправителя к получателю).

Шифрование аппаратное [hardware encryption] — *шифрование*, выполняемое с применением *средств криптографических аппаратных*.

Шифрование аппаратно-программное [hardware software encryption] — *шифрование*, выполняемое с применением *средств криптографических* аппаратно-программных.

Шифрование блочное [block encryption, block ciphering] — см. *алгоритм шифрования блочный*.

Шифрование канальное [chanel encryption, link encryption] — способ *шифрования*, при котором *шифрование* данных осуществляется в *канале связи* между двумя узлами (которые могут быть промежуточными на пути от отправителя к получателю).

Шифрование линейное [linear encryption] — способ *шифрования*, при котором *зашифрование* и *расшифрование* данных производятся непосредственно в процессе передачи (приема) информации по *каналу связи*.

Шифрование поточное [stream encryption] — см. *алгоритм шифрования поточный*.

Шифрование предварительное [primary encryption] — *шифрование* сообщения перед его отправлением по *линии связи* или перед использованием основного *криптографического алгоритма* в полном объеме.

Шифрование программное [software encryption] — *шифрование*, выполняемое только с применением *средств криптографических программных*.

Шифрование сквозное [end-to-end encryption] — см. *шифрование абонентское*.

Шифрование с открытым ключом [public-key cryptosystem, asymmetric cryptosystem, син.: алгоритм шифрования асимметричный] — см. *алгоритм шифрования асимметричный*.

Шифртекст [ciphertext, син.: сообщение зашифрованное] — результат *зашифрования открытого текста*.

Э

Экспертиза [expertise,review] — комплекс мероприятий по анализу и оценке *средств* и *систем криптографической защиты информации* на основе представленной документации и протоколов испытаний в целях получения достоверного результата о допустимости их использования для обеспечения безопасности *информации*.

Энтропия [entropy] — теоретико-информационная характеристика распределения случайной величины. Э. дискретной случайной величины S с распределением $(p_1,.., p_n,...)$ равна $H(S) = -\sum_i p_i \log p_i$.

ЛИТЕРАТУРА

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: учеб. пособие. – М. : Гелиос АРВ, 2005. – 480 с.
2. Алексей Кулыгин, МЦНМО Англо-русский и русско-английский словарь криптографических терминов // [Electronic resource] – Mode of access: http://citforum.ru/security/cryptography/dictionary/.
3. Англо-русский справочный словарь терминов по криптографии и защите информации // [Electronic resource] – Mode of access: http://www.rfcmd.ru/glossword/1.8/index.php?a=index&d=23.
4. Англо-русский криптологический словарь с толкованиями // [Electronic resource] – Mode of access: http://www.help-antivirus.ru/protectioninformation/Prilo/Index.php.
5. Аргановский С.А., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стеганоанализ (учеб. пособие для специальности «Компьютерная безопасность»). – М.: Вузовская книга, 2009.
6. Аргановский А.В., Девянин П.В., Хади Р.А., Черемушкин А.В. Основы компьютерной стеганографии. – М.: Радио и связь, 2003.
7. Вероятность и математическая статистика. Энциклопедия. Под ред. Ю.В.Прохорова. – М.: БРЭ, 1999.
8. ГОСТ ИСО/МЭК 2382-1-99. Информационная технология. Словарь. Часть 1. Основные термины. Введен 01.07.00.
9. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введен 01.07.90.
10. Гостехкомиссия России. Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Москва 1992.
11. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2002.
12. Инструкция по шифровальной службе в Республике Беларусь. Утверждена Постановлением Совета Министров РБ №1039-11 от 7 июля 1999 г.
13. Инструкция о порядке защиты информации на объектах средств вычислительной техники в Вооруженных Силах Республики Беларусь. Утверждена Постановлением Министерства обороны Республики Беларусь от 21 июня 2005года № 08.
14. Закон Республики Беларусь «Об информации, информатизации и защите информации». 10 ноября 2008 г. № 455-З.
15. Закон Республики Беларусь «О государственных секретах». 29 ноября 1994 г. № 3410-XII.
16. Закон Республики Беларусь «О государственных секретах». 19 июля 2010 г. № 170-З.
17. Закон Республики Беларусь «Об электронном документе и электронной цифровой подписи». 28 декабря 2009 г. № 113-З.
18. Концепция создания банковской инфраструктуры открытых ключей. Утверждена Постановлением Совета директоров Национального банка Республики Беларусь 19.10.2006 № 281.
19. Лукацкий А.В. Краткий толковый словарь по информационной безопасности: 1000 терминов. Москва, 2000.
20. Методика обеспечения безопасности, утвержденная Федеральным стандартом обработки информации FIPS.

21. Национальный стандарт Российской Федерации. Основные термины и определения. Защита информации. 2006.
22. Пономарев К.И., Путилов Г.П. Стеганография: история и современные технологии. – М.: МИЭМ, 2009.
23. Проект стандарта Украины «Информационные технологии. Криптографическая защита информации. Термины и определения».
24. Сборник основных терминов и определений в области защиты информации – Мн.: НИИ ВС РБ, 2010. –100 с.
25. Словарь криптографических терминов / под ред. Б.А. Погорелова, В.Н. Сачкова. – М.: МЦНМО, 2006.
26. Словарь криптографических терминов / под ред. Б.А. Погорелова, В.Н. Сачкова. // [Electronic resource] – Mode of access: http://bookre.org/reader?file=655875.
27. СТБ П 34.101.35-2009. Информационные технологии. Методы и средства безопасности. Объекты информатизации. Профиль защиты класса Б3. Введён 01.08.09.
28. СТБ 1596-2009. Информационная безопасность сети электросвязи. Термины и определения. Введен 01.01.2010.
29. СТБ 34.101.1-2004. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен 01.02.05.
30. СТБ 34.101.11-2009. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Профиль защиты операционной системы сервера для использования в доверенной зоне корпоративной сети. Введен 01.09.2009.
31. СТБ П 34.101.37-2009. Информационные технологии. Методы и средства безопасности. Профиль защиты программных средств системы управления сайта. Введен 01.09.2009.
32. СТБ П 34.101.36-2009. Информационные технологии. Методы и средства безопасности. Объекты информатизации. Профиль защиты класса А 2. Введен 01.08.2009.
33. СТБ 34.101.8-2006. Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования. Введен 01.07.2006.
34. СТБ П ISO/IEC 27001-2008. Информационные технологии. Технологии безопасности. Системы управления защитой информации. Требования. Введен 01.03.2009.
35. СТБ 34.101.30-2007. Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация. Введен 01.04.08.
36. СТБ П 34.101.38-2009. Информационные технологии и безопасность. Классификация объектов информационных технологий по требованиям информационной безопасности. Введен 01.11.2009.
37. СТБ 982-94. Информационные технологи. Термины и определения. Введен 01.07.95.
38. СТБ П ISO/IEC 18033-1-2008. Информационные технологии. Технологии безопасности. Алгоритмы шифрования. Часть 1. Общие положения. Введен 01.11.2008.

39. СТБ П 34.101.40-2009. Информационные технологии. Методы и средства безопасности. Методика оценки показателей защищенности и надежности специального программного обеспечения. Введен 01.11.2009.
40. СТБ П ISO/IEC 18033-3-2008. Информационные технологии. Технологии безопасности. Алгоритмы шифрования. Часть 3. Блочные шифры. Введен 01.11.2008.
41. СТБ ГОСТ Р 50922-2000. Защита информации. Основные термины и определения. Введен 01.01.2001.
42. СТБ П 34.101.24-2008. Информационные технологии. Электронные цифровые подписи и инфраструктуры. Требования к политике удостоверяющих центров, выдающих квалификационные сертификаты. Введен 01.03.2009.
43. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости : учебное пособие для студ. учреждений высш. проф. образования. М.: Издательский центр «Академия», 2009. – 272 с.
44. Фергюсон Н., Шнайер Б. Практическая криптография. –М.: Ид «Вильямс», 2005. – 424 с.
45. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии. – Минск/Москва: Новое Знание, 2003. – 382 с.
46. Харин Ю.С., Петлицкий А.И., Ярмола А.Н. Криптографические генераторы случайных и псевдослучайных последовательностей и методы их тестирования: Обзор. – В сб. Комплексная защита информации. – Минск: Амалфея, 2007.
47. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002.
48. Bauer F.L. Decrypted Secrets: Methods and Maxims of Cryptology. – Berlin: Springer, 1997.
49. Goldreich O. Foundations of Cryptography. Cambridge University Press, 2001. Vol. 1.
50. ISO-IEC 11770-1. Информационные технологии. Методы безопасности. Управление ключами. Часть 1. Структура.
51. ISO-IEC 11770-2. Information technology - Security techniques - Key management.
52. ISO-IEC 11770-3. Information technology - Security techniques - Key management - Part 3 Mechanisms using asymmetric techniques.
53. ISO-IEC 9798-1. Информационные технологии. Методы защиты. Механизмы аутентификации объектов. Часть 1. Общие положения.
54. ISO-IEC 10118-1. Information technology - Security techniques - Hash-functions – Part 1. General.
55. Menezes A.J., van Oorschot, Vanstone S.A. Handbook of Applied Cryptography. – CRC Press, 1997. – xxvii+780pp.
56. National Institute of Standards and Technology (NIST). FIPS Publication 140-1: Security Requirements for Cryptographic Modules, 2001.
57. National Institute of Standards and Technology (NIST). FIPS Publication 180: Secure Hash Standard (SHS), 1993.
58. National Institute of Standards and Technology (NIST). FIPS Publication 186: Digital Signature Standard (DSS), 1994.
59. National Institute of Standards and Technology (NIST). FIPS Publication 197: Advanced Encryption Standard (AES), 2001.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Д

З

И

К

Л

М

Н

О

П

Р

С

Т

У

Ф

Х

Ц

Ш

Э

M

R

S

Справочное издание

СЛОВАРЬ ОСНОВНЫХ ТЕРМИНОВ ПО КРИПТОЛОГИИ

С о с т а в и т е л и
Харин Юрий Семенович,
Герасименок Владимир Владимирович,
Матвеев Геннадий Васильевич и др.

В авторской редакции

Подписано в печать 19.03.2013. Формат 60×84/16. Бумага офсетная.
Усл. печ. л. 3,95. Уч.-изд. л. 3,05. Тираж 50 экз. Заказ

Белорусский государственный университет.
ЛИ № 02330/0494425 от 08.04.2009.
Пр. Независимости, 4, 220030, Минск.

Отпечатано с оригинала-макета заказчика
на копировально-множительной технике
факультета прикладной математики и информатики
Белорусского государственного университета.
Пр. Независимости, 4, 220030, Минск.