Глоссарий

А

Абонент [abonent, subsriber, user] — лицо (группа лиц, организация), имеющее право на пользование услугами вычислительной системы.

Абонентское шифрование (информации) — способ шифрования, при котором зашифрование данных осуществляется в системе абонента—получателя.

Абонентское шифрование (оконечное) [end-to-end encryption] — защита информации, передаваемой средствами телекоммуникаций криптографическими методами, непосредственно между отправителем и получателем.

Абстрактное представление данных — принцип определения типа данных через операции, которые могут, выполняться над объектами данного типа. При этом вводятся следующие ограничения: значения объектов могут модифицироваться и наблюдаться только путем использования этих операций

Аварийная ситуация [disaster situation] — отказ вычислительной системы, приводящий к прекращению выполнения задач.

Аварийное завершение [abnormal end (termination), abend] — прекращение выполнения задачи при возникновении условий, исключающих возможность ее дальнейшего выполнения. К таким условиям относятся аварийные сбои, грубые ошибки в программе и др. Цели завершения: выдать информацию об аварийной ситуации, освободить ресурсы, занятые задачей, сохранить работоспособность вычислительной системы, продолжить решение других задач.

Аварийный [postmortem] — определение, характеризующее анализ причин возникновения нежелательных ситуаций в работе системы, основанный на информации, записанной в момент обнаружения нежелательной ситуации.

Аварийный отказ [Crash] — отказ, требующий для возобновления нормального функционирования вычислительной системы по крайней мере, вмешательства оператора, а иногда и ремонтных работ.

Авария головки [Head chash] — случайное разрушительное соприкосновение головки считывания-записи с поверхностью жесткого диска при вращении последнего в дисководе. При аварии головки диск приходит в негодность, поскольку при контакте соответствующая дорожка и находящаяся на ней информация разрушаются.

Автоматизированная информационная система, АИС [Automated information system (AIS)] — совокупность программных и аппаратных средств, предназначенных для создания, передачи, обработки, распространения, хранения и/или управления данными и информацией и производства вычислений.

Автоматическая проверка [Automatic check] — любая непрограммируемая проверка правильности сегмента данных.

Автоматический верификатор [Mechanical verifier] — схема обеспечения автоматического доказательства правильности программ. Включает генератор условий верификаций и блок доказательства теорем.

Автоматический контроль (встроенный контроль) [Automatic check (builtin check)] — контроль, выполняемый автоматически аппаратными средствами.

Автономное (инженерное) средство защиты информации — специальное защитное сооружение, устройство или приспособление, не входящее в комплект технического средства обработки информации, а также устройство общего назначения, используемое для целей защиты.

Авторизация [Authorization] — предоставление доступа пользователю, программе или процессу.

еще — предоставление определенных полномочий лицу (группе лиц) на выполнение некоторых действий в системе обработки данных.

Авторизация данных [Data authorization] — определение и установление степени приватности данных в базе данных.

Авторизация программы [Program authorization] — установление ограничения на доступ к системной или пользовательской программе со стороны других программ и пользователей.

Авторское право — совокупность правовых норм (раздел гражданского права), которые регулируют отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), фонограмм, исполнения, постановок, передач организаций эфирного или кабельного вещания.

Администратор базы данных [Data administrator — специальное должностное лицо (группа лиц), имеющий(ие) полное представление о базе данных и отвечающее за ее ведение, использование и развитие. Входит в состав администрации банка данных.

еще — лицо, имеющее полное представление о данных, используемых в учреждении (на предприятии), и отвечающее за хранение, обновление и организацию их использования.

Администратор доступа [Access administrator] — одно из должностных лиц в составе администрации банка данных, отвечающее за организацию доступа пользователей к базам данных.

Администратор защиты [Security administrator] — субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Администратор системы (системный администратор) [Systemadministrator] — лицо, отвечающее за эксплуатацию системы и поддержание ее в работоспособном состоянии

Администратор службы безопасности — человек (или группа людей), имеющий(ие) полное представление об одной или нескольких системах обеспечения безопасности и контролирующий(ие) проектирование и их использование.

Администрация банка данных [Databank administratoin] — группа лиц (подразделение), отвечающих за эксплуатацию банка данных: ведение баз данных, организацию коллективного доступа к ним пользователей и развитие системы.

Администрация системы [System administration] — пользователь сети, деятельность которого связана с управлением системами.

Администрирование базы данных [database administration] — выполнение функций определения, организации, управления и защиты данных в базе (ДСТУ 2874).

Аккредитация [Accreditation] — авторизация и санкционирование возможности обработки критичных данных в операционной среде информационной системы или сети. Решение об аккредитации выносится после получения всеми лицами из технического персонала сертификата, подтверждающего возможность этих лиц работать с защищенными системами. При этом предварительно должно быть подтверждено соответствие проекта самой системы и его конкретной реализации набору заранее определенных технических требований. Все эти условия служат единственной цели обеспечению степени безопасности адекватной, уровню критичности данных.

Аккредитация в области защиты информации — официальное признание правомочий осуществлять какую-либо деятельность в области сертификации защищенных изделий,технических средств и способов защиты информации.

Активная угроза [Active threat] — угроза преднамеренного несанкционированного изменения состояния системы.

Активное скрытие [active hiding] — способ технической защиты информации, состоящий в повышении энергетических характеристик сигналов, полей или концентраций веществ, затрудняющем обнаружение носителей информации и ее получение.

Активное содержимое — WWW-страницы, которые содержат ссылки на программы, что загружаются и выполняются автоматически WWW-браузерами.

Активное техническое средство защиты — техническое средство защиты, обеспечивающее создание маскирующих или имитирующих активные помехи средства технической разведки или нарушение нормального функционирования этих средств. К активным техническим средствам защиты относятся ложные сооружения и объекты, макеты изделий и другие имитаторы, а также средства постановки аэрозольных и дымовых завес, устройства электромагнитного и акустического зашумления и другие средства постановки активных помех.

Активность защиты — принцип защиты, выражающийся в целенаправленном навязывании техническим раз-

ведкам ложного представления об объекте в соответствии с замыслом защиты, а также подавление возможностей технической разведки.

Акустическая защита выделенного помещения — процесс реализации запланированного комплекса организационно — технических мероприятий по предотвращению утечки речевой секретной или конфиденциальной информации за пределы выделенного помещения путем прямого проникновения звука через ограждающие конструкции.

Акустическая защищенность выделенного помещения — уровень акустической защищенности выделенного помещения, достигнутый в результате проведения акустической защиты. Уровень акустической защищенности проверяется и оценивается при проведении аттестации выделенного помещения.

Акустическая информация — информация, носителем которой являются акустические сигналы.

Акустические колебания — механические колебания частиц упругой среды, распространяющиеся от источника колебаний в окружающее пространство в виде волн различной длины. Первичными источниками акустических колебаний являются механические колебательные системы, вторичными — преобразователи различного типа, в том числе электроакустические.

Акустический сигнал — возмущение упругой среды, проявляющееся в возникновении акустических колебаний различной формы и длительности. В зависимости от формы акустических колебаний различают простые (тональные) и сложные акустические сигналы

Акустическое давление — величина колебательной силы, действующей на единичную площадь фронта волны и вызывающая периодическое сжатие и разряжение упругой среды (газа, жидкости). $P = F/S^2$, где P — акустическое давление, н/м ; F — величина колебательной силы, н; S — площадь фронта волны, м^2.

Акустическое поле — силовое поле, возникающее в упругой среде вокруг источника акустических колебаний и являющееся источником колебательной силы. Основными параметрами акустического поля являются: акустическое давление, колебательная скорость и интенсивность акустических колебаний.

Алгоритм [algorithm] — упорядоченный конечный набор четко определенных правил для решения задач за конечное количество шагов (ДСТУ 2873).

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

Алгоритмический доступ [Algorithmic access] — доступ, основанный на вычислении адреса по некоторому алгоритму.

Амортизация отказов [Fail soft] — свойство вычислительной системы, состоящее в способности распознавать изменения окружающей среды и выполнять свои функции в условиях отказа или изъятия части оборудования.

Анализ затрат (выгоды) [Costbenefit analysis] — Стадия в разработке или функционировании системы, на которой определяется стоимость обеспечения требуемого уровня защиты данных в информационной системе; иногда под этой стоимостью подразумевают ущерб, который может быть нанесен в случае утери или компрометации данных, подлежащих защите.

Анализ прерывания [Interrupt analysis] — функция, выполняемая обработчиком прерываний по коду в старом слове состояния программы (PSW) и состоящая в определении причины прерывания и выборе соответствующей программы его обработки

Анализ риска [Risk analysis] — процесс изучения характеристик и слабых сторон системы, проводимый с использованием вероятностных расчетов, с целью определения ожидаемого ущерба в случае возникновения неблагоприятных событий. Задача анализа риска состоит в определении степени приемлемости того или иного риска в работе системы.

еще — процесс определения угроз безопасности системы и отдельным ее компонентам, определения их характеристик и потенциального ущерба, а также разработка контрмер.

Анализ трафика (рабочей нагрузки) линии связи [Traffic analysis] — исследование наблюдаемых потоков данных, проходящих между пунктами посети связи (наличие, отсутствие, объем, направление, частота).

Анализатор [Analyzer] — в системах программирования алгоритм, выполняющий анализ исходной программы.

Анализатор аварийного состояния [Emergency (disaster situation) analyzer] — в СМ ЭВМ программа, пред-

назначенная для анализа аварийного состояния вычислительной системы и выдачи информации на печать.

Анализатор прерываний [Interrupt analyzer] — машинная программа, определяющая возможность возникновения конфликтов в системе в результате прерывания.

Антивирус — программа, обнаруживающая или обнаруживающая и удаляющая вирусы. Если вирус удалить не, удается, то зараженная программа уничтожается.

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

Аппаратная защита [Hardware security] — использование аппаратных средств, например, регистров границ или замков и ключей для защиты данных в ЭВМ.

Аппаратное прерывание [Hardware interrupt] — прерывание по ошибке при выполнении команды или прерывание от внешнего устройства.

Аппаратное средство защиты информации — специальное защитное устройство или приспособление, входящее в комплект технического средства обработки информации.

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.

Аппаратный контроль [Hardware check] — контроль, выполняемый встроенным для этого оборудованием.

Аппаратура засекречивания — специальные технические устройства для автоматического шифрования и дешифрования телефонных и телеграфных переговоров (сообщений).

Аппаратура технической разведки — совокупность технических устройств обнаружения, приема, регистрации, измерения и анализа, предназначенная для получения разведывательной информации. В зависимости от параметра технического демаскирующего признака, используемого технической разведкой для получения интересующих ее сведений об объекте защиты, может быть использован очень большой арсенал различных видов разведывательной аппаратуры.

Апплеты — небольшие приложения, написанные на различных языках программирования, которые автоматически загружаются и выполняются WWW-браузерами, поддерживающими апплеты

Архив [Archives] — 1) Совокупность данных или программ, хранимых на внешнем носителе, потребность в которых частично, полностью или временно отпала, но которые могут быть при необходимости использованы. 2) Совокупность данных или программ, сжатых программой архиватором.

Архитектура с мандатной адресацией — архитектура, которая охватывает как аппаратные средства, так и программное обеспечение (операционную систему) ЭВМ. Она обеспечивает более высокий уровень защиты ЭВМ в условиях мультиобработки. В архитектуре этого вида предусмотрено два типа хранимых в памяти слов: данные (включая программы) и мандаты. Программа может работать только с теми данными, на которые имеет мандаты. Мандат указывает, где находятся данные и какие виды доступа к этим данным разрешены.

Асимметричный шифр [Asymmetric cipher] — шифр, в котором ключ шифрования не совпадает с ключом дешифрирования.

Асимптотически оптимальный код [Asymptotically optimal code] — способ кодирования, предложенный для некоторого класса источников, который обладает тем свойством, что при стремлении числа сообщений к бесконечности избыточность кодирования стремится к нулю.

Асинхронное прерывание [Asynchronous system trap] — прерывание, возникновение которого не привязано к определенной точке программы. К таким прерываниям относятся внешние и прерывания, связанные с работой другого процесса.

Ассемблер [Assembler] — 1) Программа, используемая для преобразования исходной программы на языке ассемблера в машинный код или перемещаемую программу. 2) Язык ассемблера. 3) Транслятор, предназначенный для выполнения ассемблирования (ДСТУ 2873).

Атака [Attack] — нарушение безопасности информационной системы, позволяющее захватчику управлять операционной средой.

еще — попытка преодоления защиты системы. Атака может быть активной, ведущей к изменению дан-

ных, или пассивной. Тот факт, что атака была осуществлена еще, не значит, что она успешна. Степень успеха атаки зависит от уязвимости системы и эффективности защитных мер.

Атрибут [Attribute] — 1) Признак, описатель данных,-содержащий одну из характеристик данного: имя, тип, длину, количество, форму представления,систему счисления. 2) Поименованное свойство одного или нескольких объектов (ДСТУ 2874).

Атрибут файла [File attribute] — характеристика, определяющая файл: имя, размер, организация (тип), метод доступа, длина записи,тип записи и др.

Аттестат выделенного помещения — документ выдаваемый, органом по аттестации (сертификации) или другим специально уполномоченным органом, подтверждающий наличие необходимых условий, обеспечивающих надежную акустическую защищенность выделенного помещения в смоответствии с установленными нормами и правилами.

Аттестат объекта защиты — документ, выдаваемый органом по сертификации или другим специально уполномоченным органом, подтверждающим наличие на объекте защиты необходимых и достаточных условий для выполнения установленных требований и норм эффективности защиты информации.

Аттестация — оценка на соответствие определенным требованиям. С точки зрения защиты аттестации подлежат объекты, помещения, технические средства, программы, алгоритмы на предмет соответствия требованиям защиты информации по соответствующим классам безопасности.

Аттестация выделенного помещения — официальное подтверждение органом по аттестации (сертификации) или другим специально уполномоченным органом наличия необходимых и достаточных условий, обеспечивающих надежную акустическую защищенность выделенного помещения в соответствии с установленными нормами и требованиями. По результатам аттестации выделенному помещению устанавливается группа защищенности.

Аттестация защиты — подтверждение уполномоченным компетентным лицом, что оценка защиты была сделана квалифицировано и в соответствии с необходимыми правилами.

Аттестация объекта защиты — официальное подтверждение органом по сертификации или другим специально уполномоченным органом наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований и норм эффективности защиты информации.

Аттестация предприятий — комплекс организационно-технических мероприятий, в результате которых посредством специального документа — "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России или другими органами государственного управления в пределах их компетенции.

Аттестация программы [Program validation] — авторитетное подтверждение качества программы по общепринятой или официальной процедуре; комплекс проверок, обеспечивающий получение гарантии соответствия программы своему назначению.

Аттестация средств защиты [Endorsment] — удостоверение степени соответствия требованиям к данному классу средств защиты.

Аутентификатор — средство аутентификации, представляющее отличительный признак пользователя. Средствами аутентификации пользователя могут быть дополнительные кодовые слова, биометрические данные и другие отличительные признаки пользователя, которые вводятся в ЭВМ с клавиатуры дисплея, с идентификационной карты или при помощи специального устройства аутентификации по биометрическим данным.

Аутентификация [Authenticate] — проверка идентификации пользователя (проверка подлинности), устройства или другого компонента в системе, обычно для принятия решения о разрешении доступа к ресурсам системы; проверка целостности хранящихся или передающихся данных для обнаружения их несанкционированной модификации.

еще — проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

еще — установление (подтверждение) подлинности лиц (людей), технических и программных средств, элементов баз данных, сообщений.

Аутентификация данных (цифровая подпись) — процесс подтверждения подлинности (отсутствия фальсификации или искажения) произвольных данных, предъявленных в электронной форме. Данные могут представлять собой: сообщения, файл, элемент базы данных (программы), идентификатор (аутентификатор) пользователя, адрес сетевого абонента и т.п.

Аутентификация источника данных [Data origin authentication] — подтверждение подлинности источника полученных данных.

Аутентификация пользователя [Authentication of user] — подтверждение подлинности пользователя с помощью предъявляемого им аутентификатора.

еще — проверка соответствия пользователя предъявляемому им идентификатору.

Аутентификация сообщений [Authentication of messages] — добавление к блоку данных контрольного поля для обнаружения любых изменений в данных. При вычислении значений этого поля используется ключ, известный только приемнику данных.

Б

База данных [database] — совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ. Является информационной моделью предметной области. БД, как правило, представляются тремя уровнями абстракции: внешним, концептуальным и внутренним. Соответственно уровням различают внешнюю, концептуальную и физическую модели (схемы) БД. 0бращение к БД осуществляется с помощью системы управления базами данных.

еще — совокупность взаимосвязанных данных, организованных в соответствии со схемой базы данных таким образом, чтобы с ними мог работать пользователь (ДСТУ 2874).

Банк данных [Databank] — автоматизированная информационная система централизованного хранения и коллективного использования данных. В состав банка данных входят одна или несколько баз данных, справочник баз данных, система управления базами данных, а также библиотеки запросов и прикладных программ.

еще — система, предоставляющая услуги по хранению и поиску данных определенной группе пользователей по определенной тематике.

Безопасная операционная система [Secure operating system] — операционная система, эффективно управляющая аппаратными и программными средствами с целью обеспечения уровня защиты, соответствующего содержанию данных и ресурсов, контролируемых этой системой.

Безопасное время [Security time] — математическое ожидание времени раскрытия системы защиты статистическим опробированием возможных вариантов доступа к данным. Вычисляется по формуле: $T = \sum_{i=1}^{n} p_i t_i$ где n — число проб, p_i — вероятность раскрытия при i-й пробе, t_i — время, затрачиваемое на l-ю пробу.

Безопасное состояние [secure state] — условие, при выполнении которого ни один субъект не может получить доступ ни к какому объекту иначе как на основе проверки имеющихся у него полномочий.

Безопасность [Safety (security)] — свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные ее состояния или поведение.

еще — состояние, в котором файлы данных и программы не могут быть использованы, просмотрены и модифицированы неавторизованными лицами (включая персонал системы), компьютерами или программами. Безопасность обеспечивается путем создания вокруг компьютера и оборудования защищенной зоны, в которой работает только авторизованный персонал, а также использования специального программного обеспечения и встроенных в операционные процедуры механизмов защиты.

Безопасность автоматизированной информационной системы [Automated information system security] — совокупность мер управления и контроля, защищающая APIS от отказа в обслуживании и несанкционированного (умышленного или случайного) раскрытия, модификации или разрушения АИС и данных.

Безопасность данных [Data security] — защита данных от несанкционированной (случайной или намеренной) модификации, разрушения или раскрытия.

еще — свойство компьютерной системы противостоять попыткам несанкционированного доступа к обрабатываемой и хранимой информации. Безопасность достигается применением аппаратных, программных и криптографических методов и средств защиты, а также комплексом организационных мероприятий. Одним из показателей безопасности является безопасное время.

Безопасность информации [Information security] — состояние информации, при котором исключаются случайные или преднамеренные несанкционированные воздействия на информацию или несанкционированное ее получение.

еще — состояние уровня защищенности информации при ее обработке техническими средствами, обеспечивающее сохранение таких ее качественных характеристик (свойств) как секретность (конфиденциальность), целостность и доступность.

еще — состояние защищенности информации, обрабатываемой средствами вычислительной техники, или автоматизированной системы от внутренних или внешних угроз.

Безопасность информации в ИС — защищенность информации и оборудования ИС от факторов, представляющих угрозу для: конфиденциальности (обеспечение санкционированного доступа); целостности; доступности.

Безопасность информационная — способность системы противостоять случайным или преднамеренным, внутренним или внешним информационным воздействиям, следствием которых могут быть ее нежелательное состояние или поведение.

Безопасность информационной сети [Network security] — меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов.

Безопасность информационной системы [Information system security] — свойство информационной системы противостоять попыткам несанкционированного доступа. Совокупность элементов, необходимых для обеспечения адекватной защиты компьютерной системы; включает аппаратные и/или программные функции, характеристики и средства; операционные и учетные процедуры, средства управления доступом на центральном компьютере, удаленных компьютерах и телекоммуникационных средствах; административные мероприятия, физические конструкции и устройства; управление персоналом и коммуникациями.

Безопасность компьютерных систем [Computer security] – свойство компьютерных систем противостоять попыткам несанкционированного доступа к обрабатываемой и хранимой информации, вводу информации, приводящей к деструктивным действиям, и навязыванию ложной информации.

Безопасность персонала [Personnel security] — метод обеспечения гарантий того, что весь персонал, имеющий возможность доступа к некоторой критичной информации, обладает необходимой авторизацией, равно как и всеми необходимыми разрешениями.

Безопасность предприятия — стабильно прогнозируемое во времени состояние окружения, в котором предприятие может осуществлять свои действия без нарушений и перерывов.

Безопасность реальной открытой системы [Data processing systemsecurity] — технологические и административные охранные меры, применяемые в реальной открытой системе для защиты оборудования, программного обеспечения и данных от случайных и преднамеренных модификаций, раскрытия и разрушения.

Безопасность связи [Communication security] — свойство систем связи противостоять попыткам несанкционированного доступа к обрабатываемой и хранимой информации, вводу информации, приводящей к деструктивным действиям, навязыванию ложной информации.

Безопасность, информационная государства — то же, что и "безопасность, информационная объекта" применительно к государству.

Безопасность, информационная личности — то же, что и "безопасность информационная" применительно к отдельному человеку. Гарантирует защиту от сбора, хранения, использования и распространения информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписи, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения.

Безопасность, информационная общества — то же, что и "безопасность, информационная личности" применительно к организованному коллективу людей и к обществу в целом.

Безопасность, информационная объекта — состояние объекта при котором обеспечивается: 1) высокоэффективное информационное обеспечение всех видов его деятельности; 2) надежная защита всей существенно значимой информации; 3) надежная защита от негативного воздействия информации на объект или его составные компоненты.

Безотказность — способность системы выполнять возложенные на нее функции в требуемый момент времени в задаваемых условиях.

Белый (акустический) шум — сложный акустический сигнал, имеющий постоянную спектральную плотность во всем диапазоне частот.

Биометрические данные — средства аутентификации, представляющие собой такие личные отличительные

признаки пользователя как тембр голоса, форма кисти руки, отпечатки пальцев и т.д., оригиналы которых в цифровом виде хранятся в памяти ЭВМ.

Бит (двоичный код) [Bit] — минимальная единица количества информации в ЭВМ, равная одному двоичному разряду.

Бит достоверности [Validity bit] — разряд, добавляемый к слову в памяти ЭВМ для указания достоверности информации.

Бит защиты [Protection bit] — двоичный разряд в ключе памяти, устанавливающий защиту соответствующего блока памяти от записи либо отвыборки и записи.

Бит контроля на четность (бит четности, контрольный бит) [Paritychecknbit] — контрольный бит, добавляемый к данным для контроля их верности таким образом, чтобы сумма двоичных единиц, составляющих данное, включая и единицу контрольного бита, всегда была четной (либо всегда нечетной).

Бит маски [Mask bit] — сочетание битов, устанавливаемых в нулевое или единичное значение для разрешения или запрета определенных операций либо для проверки или изменения содержимого поля.

Бит управления доступом [Access control bit] — один из нескольких битов ключа памяти, сопоставляемых с ключом защиты при обращении к соответствующему блоку памяти с целью организации ее защиты.

Блок доступа к записи [Record access block (RAB)] — в СМ ЭВМ структура данных в системе управления данными (СУД), содержащая запрос на доступ к записи файла СУД.

Блок доступа к файлу [File access block (FAB)] — в СМ ЭВМ структура данных, используемая системой управления данными (СУД) для выполнения операций над файлами с последовательной, относительной или индексной организациями и содержащая основные данные о файле.

Блок контроля и диагностики — устройство, выполняющее аппаратным способом функции проверки работоспособности отдельных устройств и диагностику обнаруженных ошибок с целью устранения неисправностей.

Блок начальной загрузки [Bootstap block] — блок магнитного диска, автоматически считываемый при запуске системы и содержащий программу загрузки с этого диска остальной части системы.

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

Блокировка данных [Data interlock] — защита файла или его части (блока,записи) путем запрещения доступа к ним всех пользователей, за исключением одного.

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

Блокировка записи в память [Read lockout] — ситуация при обменеданными, характеризующаяся тем, что запись, читаемая с внешнего носителя, в основную память не переводится.

Блокировка клавиатуры [Keyboard lockout] — запрет на ввод данных в ЭВМ с клавиатуры терминала. Выполняется операционной системой. Причинами блокировки могут быть занятость ресурсов ЭВМ, машинные сбои, ошибки в программном обеспечении и др.

Блокировка памяти [Memory lockout] — запрещение доступа к ограниченному участку памяти, например, дорожке диска, вследствие обнаруженных на этом участке дефектов. Выполняется программными или аппаратными средствами.

Блочный алгоритм шифрования — алгоритм шифрования, осуществляющий криптографическое преобразование исходной информации путем выполнения криптографических операций над n-битными блоками открытого текста.

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

еще — является защитным барьером, состоящим из нескольких компонентов (например, маршрутизатора или шлюза, на котором работает программное обеспечение брандмауэра). Брандмауэр конфигурируется в соответствии с принятой в организации политикой контроля доступа к внутренней сети. Все входящие и исходящие пакеты должны проходить через брандмауэр, который пропускает только авторизованные пакеты.

Брандмауэр с фильрацией пакетов [packet-filtering firewall] — является маршрутизатором или компью-

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

Брандмауэр экспертного уровня [stateful inspecthion firewall] — проверяет содержимое принимаемых пакетов на трех уровнях модели OSI — сетевом, сеансовом и прикладном. Для выполнения этой задачи используются специальные алгоритмы фильтрации пакетов, с помощью которых каждый пакет сравнивается с известным шаблоном авторизованных пакетов.

Браузер — клиентская программа для работы в WWW.

Брешь безопасности [security flaw] — ошибка при назначении полномочий или упущение при разработке, реализации или управлении средствами защиты системы, которые могут привести к преодолению защиты.

В

Ведение базы данных [Database maintenance] — деятельность, направленная на обновление и восстановление базы данных, а также на перестройку ее структуры) (ДСТУ 2874).

Ведение контроля [Auditing] — процедуры управления. системой, необходимые для обеспечения нормальной работы системы и выполнения имеющихся задач, а также для обеспечения эффективности работы и эффективности использования ресурсов информационной системы. Ведение контроля может осуществляться лицами, отличными от лиц, непосредственно отвечающих за работу системы и решение конкретных задач.

Векторное прерывание [Vectored interrupts] — эффективный метод прерывания, реализуемый аппаратно при работе с множеством разнотипных устройств, каждое из которых способно формировать сигналы прерывания, причем для каждого устройства требуется своя уникальная программа обработки прерываний. Вектор прерываний это массив адресов таких программ. При успешном выполнении прерывания процессора устройство сообщает процессору адрес точки входа в вектор прерываний. Процессор использует этот адрес для передачи управления соответствующей программе обработки прерывания.

Верительные данные [Credentials] — данные для установления подлинности личности, за которую выдает себя пользователь ресурса ВОС.

Верификатор условий [Assertion checker] — программа, анализирующая текст другой программы, снабженной условиями и операторами контроля, которые должны выполняться в определенных ее точках, и доказывающая их истинность или ложность при заданных предусловиях.

Верификация [verification] — процесс сравнения двух уровней спецификации средств вычислительной техники или их комплексов на надлежащее соответствие.

еще — в программировании доказательство правильности программ. Различают два подхода к верификации: статические и конструктивные методы.

еще — процесс сопоставления двух уровней спецификаций системы (например, модели политики безопасности и спецификаций системы, спецификаций системы и исходных кодов, исходных кодов и выполняемых кодов) для установления необходимого соответствия между ними. Этот процесс может быть полностью или частично автоматизирован.

Верификация и подтверждение правильности [Verification andvalidation (V & V)] — общий термин для обозначения полного набора проверок, которым подвергается система для получения гарантий ее соответствия своему назначению. В число таких проверок могут входить жесткий набор функциональных тестов, контроль пропускной способности, проверка надежности и т. д.

Верификация программ [Program verification] — любой метод, который убеждает в том, что программа будет выполнять именно то, что от нееожидается.

еще — доказательство того, что поведение программы соответствует \спецификации на эту программу (ДСТУ 2873).

Вертикальная маска — маска, предназначенная для скрытия (маскировки) объекта защиты от наблюдения сбоку (от наземной или перспективной воздушной разведок).

Взвешенный код [Weighted code] — блочный код, в котором каждой позиции символа в закодированном слове присваивается определенный вес.

Взрыв [Blowup] — в вычислительных системах аварийный останов с выдачей сообщения об ошибке, блокирующий дальнейшее выполнение программы.

Вибрационный (структурный) канал утечки акустической (речевой) информации — канал утечки акустической (речевой) информации, средой распространения акустических сигналов в котором являются ограждающие конструкции зданий, сооружений и другие твердые тела.

Виброакустический канал утечки акустической (речевой) информации — канал утечки акустической (речевой) информации, обусловленный распространением механических колебаний из твердой среды в воздушную и возбуждениесм последней.

Вибростойкость технического средства обработки информации — устойчивость технического средства обработки информации против вибраций, вызываемых стихийными бедствиями (землетрясениями, ураганами и т,д,).

Визуальный контроль [Sight check] — контроль программы и данных на бланках, перфокартах или экране дисплея, выполняемый программистом методом просмотра.

Вирус [Virus] — небольшая программа, которая вставляет саму себя в другие программы при выполнении.

еще — программа, способная самопроизвольно создавать свои копии и модифицирующая другие программы, записанные в файлах или системных областях, для последующего получения управления и воспроизводства новой копии. Часто содержит логические бомбы или создает различные аудио и видео эффекты. Переносится при копировании программ либо через дискеты, с которыми работали на зараженном компьютере.

Вирус невидимка [Stealth virus] — вирус, использующий специальные алгоритмы, маскирующие его присутствие на диске (в некоторых случаях в оперативной памяти).

Владелец [Owner] — в системе защиты данных и контроля доступа пользователь, имеющий неограниченные права по отношению к файлу или другой информации.

Владелец информации — субъект информационных отношений, обладающий правом владения, распоряжения и пользования информационным ресурсом по договору с собственником информации.

Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных Законом.

Внешнее воздействие на информационный ресурс — фактор опасности, вызываемый стихийными бедствиями, мощными электромагнитными излучениями или диверсионными актами и приводящий к нарушению целостности информации или ее блокированию.

Внешняя схема базы данных [external schema] — Формальное описание базы данных на внешнем уровне в соответствии с конкретной моделью данных.

Внутренняя схема базы данных [internal schema] — формальное описание базы данных на внутреннем уровне в соответствии с конкретной моделью данных.

Военно-промышленный объект — групповой объект защиты, функциональная деятельность которого связана с разработкой, изготовлением, испытанием и эксплуатацией образцов вооружения и военной техники, а также с другими вопросами оборонной тематики, сведения о которых требуют защиты от технических разведок.

Военный объект — групповой объект защиты, функциональная деятельность которого связана с испытанием или эксплуатацией образцов вооружения и военной техники силами войск.

Воздушный канал утечки акустической (речевой) информации — канал утечки акустической (речевой) информации, средой распространения акустических сигналов в котором является воздух. Воздушная среда может обычной атмосферной или искусственно созданной газовой средой. В соответствии с этим различают атмосферный и газовый каналы утечки акустической (речевой) информации.

Возможности технической разведки — характеристики способности обнаружения, распознавания, измерения и регистрации технических демаскирующих признаков объекта средствами технической разведки.

Восстанавливаемая система [Recovery system] — система, допускающая ремонт в процессе выполнения своих функций.

Восстанавливаемость [Recoverability (refreshable)] — свойство загружаемого модуля, состоящее в возможности защиты его в процессе выполнения от модификации как им самим, так и любым другим модулем. Программа восстановления может заменить такой модуль новым экземпляром, не повлияв при этом ни на порядок обработки, ни на конечный результат.

Восстановительные процедуры [recovery procedures] — действия, предпринимаемые для восстановления способности системы обрабатывать информацию, а также восстановление наборов данных после аварии или сбоя.

Восстановление [Recovery (regeneration)] — 1) Возврат к исходному значению или к нормальному функционированию. 2) Процесс, с помощью которого станция передачи данных разрешает конфликт или исправляет ошибки, возникающие при передаче данных.

Восстановление базы данных [database recovery] — 1) Полная или частичная повторная загрузка базы данных (ДСТУ 2874). 2) Воссоздание содержимого базы данных по резервной копии, выполняемое в случае машинных сбоев или программных ошибок для поддержания целостности данных. Методами и средствами восстановления являются: копирование, рестарт сконтрольной точки, системный журнал.

Восстановление данных [Data recovery] — процесс копирования данных с носителя, содержащего защитную копию данных, на носительоригинал в случае нарушения на нем целостности данных.

Восстановление после отказа [Failure recovery] — процедура возобновления работы вычислительной системы после отказа, исключающая выработку системой неверных результатов.

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

Восстановление при ошибках [Error recovery] — способность программы или системы продолжать работу после обнаружения ошибки.

Восстановление сети [Network security] — совокупность действий, выполняемых для восстановления работоспособности вычислительной сети.

Восстановление синхронизации [Clock recovery] — в вычислительных сетях выделение тактовых сигналов из сигналов, принимаемых в синхронном режиме.

Восстановление синхронизации в кодировании [Synchronization recovery] — установка декодера на начало некоторого кодового слова.

Восстановление файла [File recovery] — процесс восстановления целостности файла после обнаружения в нем ошибок.

Временная противоречивость [Temporary inconsistency] — кажущаяся противоречивость данных в базе данных, возникающая для одной программы, если вторая в это время выполняет обновление данных. Так, если первая программа читает и суммирует данные, в то время как вторая еще не завершила их обновление, полученная сумма будет представлять собой искаженный результат.

Время восстановления [Recovery time] — время между моментом обнаружения сбоя и моментом возобновления работы системы (устройства) после восстановления.

Время доступа (обращения) [Access time] — интервал времени между моментом выдачи команды на ввод-вывод данных и моментом начала обмена.

Время жизни [Life time] — интервал выполнения программы, в котором программный объект (например, переменная) сохраняет свое значение.

Время ремонта [Repair time] — время (иногда среднее), необходимое для диагностирования и устранения неполадок либо в технических средствах, либо в программном обеспечении вычислительной системы. В сочетании со средним временем ремонта и средним временем безотказной работы характеризует системную надежность или период работоспособного состояния системы.

Вспомогательные технические средства [auxiliary technical facilities] — средства и системы формирования, передачи, приема, преобразования, отображения и хранения открытой информации, средства и системы жизнеобеспечения различного назначения, которые могут создавать технические каналы утечки информации.

Вспомогательные технические средства и системы (ВТСС) — технические средства и системы, которые непосредственно не задействованы для обработки информации, но находятся в электромагнитном поле побочных излучений технических средств обработки информации, в результате чего на них наводится опасный сигнал, который по токопрово-

дящим коммуникациям может распространяться за пределы контролируемой зоны. К ВТСС относятся средства и системы связи, пожарной и охранной сигнализации, электрочасофикации, радиофикации, электробытовые приборы и другие вспомогательные технические средства и системы. ВТСС играют роль так называемых "случайных антенн".

Вставка [Insertion] — операция добавления к множеству (массиву, списку, файлу) нового элемента.

Вставка в программу (заплата) [Patch] — изменение в программе, которое важно внести наиболее удобным и быстрым способом, обращая меньше внимания на защиту данных ради временного восстановления работоспособности программы с целью последующего ее исправления. Часто на этапе тестирования незначительные ошибки исправляются с помощью заплат, что бы без долгих задержек продолжить тестирование, не компилируя программу каждый раз повторно. Впоследствии все необходимые изменения вносятся в исходный текст программы, которая затем компилируется повторнотолько один раз.

Встроенный дешифратор [Onchip decoder] — дешифратор, расположенный на одном и том же кристалле с запоминающей матрицей.

Вторичный индекс [secondary index] — индекс для вторичных ключей (ДСТУ 2874).

Вторичный ключ [Second key] — 1)Способ защиты программного обеспечения, в котором первый криптографический ключ открывает доступ ковторому ключу, являющемуся ключом для дешифрования программного обеспечения. 2) Ключ, который может идентифицировать более одной записи (ДСТУ 2874).

Выделенное помещение — специальное помещение, предназначенное для проведения собраний, совещаний, бесед и других мероприятий речевого характера по секретным или конфиденциальным вопросам. Мероприятия речевого характера могут проводиться в выделенных помещениях как с использованием технических средств обработки речевой информации (ТСОИ), так и без них.

Вызов [Call (calling)] — действие по активизации машинной программы,

Вычислительная сеть (сеть ЭВМ) [Network] — система взаимосвязанных между собой ЭВМ, а также технического и программного обеспечения для их взаимодействия.

Г

Гамма шифра — псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму для зашифрования открытой информации и расшифрования зашифрованной.

Гаммирование — процесс наложения по определенному закону гаммы шифра на открытые данные.

Гарантии [Assurance] — мера доверия архитектуре и средствам обеспечения безопасности системы относительно корректности и аккуратности проведения политики безопасности.

Гарантированность механизмов обеспечения ЗИ — оценка адекватности используемых механизмов обеспечения ЗИ выбранным функциональным требованиям. Гарантированность определяется эффективностью и корректностью механизмов обеспечения ЗИ.

Гарантия защиты [Security accredidation] — наличие сертификата соответствия для технического средства обработки информации или аттестата на объект информатики, подтверждающих, что безопасность обрабатываемой информации соответствует требованиям стандартов и других нормативных документов.

еще — формальное разрешение на возможность использования для работы данной конкретной вычислительной машины на месте ее установки только после обеспечения защиты от несанкционированного доступа.

Гашение изображения [Blanking, display suppression] — 1) Подавление визуализации одного или более примитивов вывода или сегментов. 2) Стирание содержимого экрана дисплея, выполняемое аппаратным путем (клавишей) или программными средствами.

Генератор [Generator] — 1) Тип транслятора, входным языком которого является проблемноориентированный язык (например, язык РПГ). 2) Составная часть транслятора, выполняющая генерацию машинных команд.

Генератор случайных паролей [Randompassword generator] — программноаппаратное средство, представляющее собой генератор случайных чисел, используемых в качестве паролей.

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

Гидроакустический канал утечки акустической (речевой) информации — канал утечки акустической (речевой) информации, средой распространения акустических сигналов в котором является жидкая (водная) среда.

Главный пароль [Master password] — 1) Корневое слово, являющееся общим для определенного набора паролей. 2) Пароль, предназначенный для защиты каталога паролей.

Государственная тайна — сведения, охраняемые государством, разглашение которых может оказать отрицательное воздействие на качественное состояние военно-экономического потенциала страны или повлечь другие тяжкие последствия для ее обороноспособности, государственной безопасности, экономических и политических интересов. К государственной тайне относится секретная информация с грифами "особой важности" и "совершенно секретно".

Готовность системы [System availability] — мера способности системы выполнять свои функции при нахождении в рабочем состоянии. Количественно готовность можно оценивать с помощью коэффициента готовности.

Граница кодирования [Coding bound] — предел производительности кода, зависимый от таких параметров, как мощность кода, минимальное расстояние Хемминга, длина кодовой комбинации.

Группа акустической защиты (защищенности) выделенного помещения — соответствие запланированного (достигнутого) уровня акустической защиты (защищенности) выделенного помещения установленным нормам в зависимости от грифа секретности защищаемой речевой информации.

Групповой объект защиты — структурное объединение единичных объектов как требующих так и не требующих защиты, предназначенных для совместного выполнения определенных функций. К групповым объектам защиты относятся режимные предприятия и учреждения, военные и военно — промышленные объекты, а также конструкторское бюро, опытные производства, испытательные полигоны, базы, аэродромы и другие объекты, связанные с разработкой, испытанием и эксплуатацией секретных изделий.

Д

Данные [data] — информация, представленная в формализованном виде, пригодном для передачи, интерпретации или обработки с участием человека либо автоматическими средствами (ДСТУ 2874).

Датчик случайных чисел — аппаратно реализованное устройство (элемент, блок), преднаназначенное для генерации случайных битовых последовательностей, обладающих необходимыми свойствами равновероятности порождаемой ключевой гаммы.

Двоичный код с исправлением ошибок [Binary errorcorrection code] — двоичный код, избыточность которого обеспечивает автоматическое обнаружение и исправление ошибок некоторых типов в передаваемых данных.

Двудомный шлюз [Dual-homed gateway] — компьютер, на котором работает программное обеспечение брандмауэра и который имеет две сетевые интерфейсные платы: одна подключена к внутренней сети, а другая — к внешней. Шлюз передает информацию из одной сети в другую, исключая прямое взаимодействие между ними. Шлюзы сеансового и прикладного уровня относятся к двудомным шлюзам.

Дезинформация [Misinformation] — сознательное искажение передаваемых сведений с целью ложного представления у лиц, использующих эти сведения; передача ложной информации.

Декодирование [Decoding] — преобразование данных в исходную форму, которую они имели до кодирования; операция, обратная кодированию.

Демон [Demon] — программа, которая контролирует работу другой программы и время от времени прерывает ее работу, не разрушая саму программу (чаще всего это программа управления периферийными устройствами).

Дескриптор [Descriptor] — описатель, элемент информационной структуры объекта, указывающий, в каком виде запоминается та или иная информация (например, в массиве записи или файле). Обратившись к дескриптору, программа получает возможность интерпретировать характеризуемые им данные.

Дешифратор (декодер) [Decjder] — логическая схема, преобразующая nразрядное входное двоичное слово (код, шифр) в единичный сигнал на одном из 2n выходов этой схемы. Обратную функцию выполняет шифратор.

Дешифратор адреса [Address decoder] — преобразователь адреса в управляющие сигналы, направляемые запоминающему устройству.

Дешифрование [Decipherement] — операция, обратная шифрованию и связанная с восстановлением исходного текста из зашифрованного.

Диагностика [diagnostics] — контроль, проверка и прогнозирование состояния объектов. Цель технической диагностики обнаружение неисправностей и выявление элементов, ненормальное функционирование которых является причиной возникновения неисправностей.

Диагностика неисправностей (отказов) [Fault diagnostics] – поиск места неисправности в ЭВМ или внешних устройствах, определение характера неисправности и установление причин ее возникновения.

Диагностика ошибок [Error diagnostics] — поиск места ошибки в программе, установление характера и причин возникновения ошибки и определение мер по ее устранению. При обнаружении ошибки выдается диагностическое сообщение.

Диагностическая программа [diagnostic program] — программа, предназначенная для обнаружения, локализации и описания неисправностей технического оборудования или ошибок программ (ДСТУ 2873).

Дискреционное управление доступом [Discretionary access control] — концепция (модель) доступа к объектам по тематическому признаку, при которой субъект доступа с определенным уровнем полномочий может передать свое право любому другому субъекту.

еще — разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать. Это право любому другому субъекту.

Диспетчер доступа (ядро защиты) — совокупность программных и аппаратных средств контроля доступа субъектов к информационным ресурсам в соответствии с установленными правилами, защищенная от внешних воздействий.

Длина кодового ограничения сверточного кода [Constraint length] — количество информационных подблоков, от которых зависит текущий кодовый подблок на выходе сверточного кодера.

Доверительность [Trusted funcionality] — свойство соответствия безопасности некоторым критериям.

Документ — форма существования информации в виде тестовых и графических материалов, выполненных любыми способами, а также в виде перфорированных и магнитных носителей, фото — и кинопленок. Текстовые и графические материалы могут быть написаны от руки, нарисованы, выгравированы, начерчены, напечатаны на машинке или исполнены типографским способом.

Документированная информация (документ) — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Домен безопасности [Secyrity domain] — ограниченная группа объектов и субъектов безопасности, к которым применяется одна методика безопасности со стороны одного и того же администратора безопасности.

Дополнительное кодовое слово — средство аутентификации, представляющее собой кодовое слово, которое запрашивается у пользователя дополнительно после предъявления пароля. Дополнительные кодовые слова могут представлять собой ответы на такие вопросы, которые едва ли известны нарушителю правил доступа. Например, год рождения отца (матери), имя племянника сестры и т.д.

Дополнительный бит [Additional bit] — бит, добавляемый к слову данных с определенной целью (например, для кадрирования или контроля на четность).

Достоверная Вычислительная База; ДВБ [Trusted Computing Base; TCB] — совокупность защитных механизмов вычислительной системы, включая программные и аппаратные компоненты, ответственные за поддержание политики безопасности. ДВБ состоит из одной или нескольких компонентов, которые вместе отвечают за реализацию единой политики безопасности в рамках системы. Способность ДВБ корректно проводить единую политику безопасности зависит в первую очередь от механизмов самой ДВБ, а так же от корректного управления со стороны администрации системы.

Достоверное программное обеспечение [Trusted software] — программное обеспечение, входящее в ДВБ (TCB).

Достоверность [Validity, adequacy] — свойство информации быть правильно воспринятой; вероятность отсутствия ошибок.

еще — степень соответствия данных, хранимых в памяти ЭВМ или документах, реальному состоянию отображаемых ими объектов предметной области.

Достоверность обработки информации [Data processing validity] — функция вероятности ошибки, т.е. события, состоящего в том, что информация в системе не совпадает в пределах заданной точности с некоторым ее истинным значением.

Достоверность передачи информации [Data transmission validity] — соответствие принятой информации переданной.

Достоверный маршрут [Trusted path] — механизм, с помощью которого пользователь за терминалом может взаимодействовать непосредственно с ДВБ (TCB). Он может быть активизирован только пользователем или ДВБ, его работа не может быть прервана, имитирована или нарушена недостоверным программным обеспечением.

Доступ [access] — предоставление данных системе обработки данных или получение их из нее путем выполнения операций поиска, чтения и (или) записи данных (ДСТУ 2874).

еще — взаимодействие между субъектом и объектом, обеспечивающее передачу информации между ними.

еще — в вычислительной технике процедура установления связи с запоминающим устройством, размещенным на нем файлом для записи или чтения данных.

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

Доступ к информации — процесс ознакомления с информацией, ее документирование, модификация или уничтожение, осуществляемые с использованием штатных технических средств.

еще — ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Доступ к файлу [File access] — просмотр, модификация, замена или удаление файла, а также просмотр и манипулирование его атрибутами.

Доступность [Availability, accessibitity] — свойство ресурса ВОС, заключающееся в возможности его использования по требованию пользователя, имеющего соответствующие полномочия.

Доступность данных [availability of data] — такое состояние данных, когда они находятся в виде, необходимом пользователю; в месте, необходимом пользователю, и в то время, когда они ему необходимы.

еще — свойство данных, состоящее в возможности их чтения пользователем или программой. Определяется рядом факторов: возможностью работать за терминалом, обладанием пароля, знанием языка запросов и т.д.

Доступность информации — свойство информации при ее обработке техническими средствами, обеспечивающее беспрепятственный доступ к ней для проведения санкционированных операций по ознакомлению, документированию, модификации и уничтожению.

Дыра [Loophole] — в вычислительной технике недоработки, ошибки в программном обеспечении или аппаратуре, позволяющие обойти процессы управления доступом.

Е

Единичный объект защиты — конкретный носитель секретной или конфиденциальной информации, представляющий собой единое целое и предназначенный для выполнения определенных функций. К единичным объектам (субъектам) защиты относятся люди, владеющие секретной или конфиденциальной информацией, секретные и конфиденциальные документы и изделия, в том числе технические средства обработки информации, выделенные здания и помещения, а также вспомогательные технические средства и системы, подверженные влиянию информационных физических полей.

Ж

Живучесть [Viability] — свойство системы оставаться работоспособной в условиях внешних воздействий.

Живучесть программного изделия [Program viability] — показатель качества программного изделия, характеризующий его способность сохранять нормальное функционирование при машинных сбоях или частичном выходе оборудования из строя.

Журнал [Journal, log] — в вычислительной технике набор данных (файл), используемый операционной или иной системой для сбора и учета статистической информации, различных сообщений и других данных.

Журнал восстановления [Recovery log] — журнал, обеспечивающий возможность восстановления базы данных или файла. Содержит информацию о всех изменениях в Б.Д. (файле) с того момента, когда было установлено, что данные достоверны и была сделана последняя резервная копия.

Журнал ошибок [Journalizing] — файл, в который система записывает информацию о сбоях.

Журнализация [Journalizing] — процесс записи в системный журнал информации о сообщениях, запросах, выполнявшихся программах, использованных наборах данных и других сведений.

З

Заверение [Notalization] — регистрация данных у доверенного третьего лица для дальнейшей уверенности в правильности таких характеристик, как содержание, источник данных, время доставки.

Зависание программы [Program hangup] — непредусмотренный останов программы, обусловленный, например, такими причинами, как попытка обращения к устройству, не подключенному к процессору.

Зависание системы [System quiescing] — останов ("замораживание") мультипрограммной системы путем подавления ввода новых заданий.

Заградительная помеха — помеха, ширина спектра частот которой значительно превышает полосу частот приемного устройства аппаратуры разведки или технического демаскирующего признака.

Загрузка базы данных [database loading] — передача данных в базу данных (ДСТУ 2874).

Загрузка по линии связи [Downline loading, download] – пересылка программного обеспечения по линии связи от одной компьютерной системы в другую, например, от центральной ЭВМ к персональному компьютеру.

Загрузочный вирус [Boot virus] — вирус, заражающий загрузочные части жестких и/или гибких дисков. Применительно к ОС MSDOS это главная загрузочная запись и загрузочный сектор.

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

Задержка синхронизации [Synchronizing delay] — количество символов кодовой последовательности, полученной после кодирования последовательности сообщений источника синхронизируемым кодом, которые требуется исследовать декодеру для того, чтобы найти начало некоторого кодового слова, т.е. восстановить синхронизацию.

Заземляющее устройство — устройство, предназначенное для снижения уровня побочных электромагнитных излучений технических средств обработки информации и наводок от них путем соединения металлических корпусов (экранов) изделий, экранирующих оплеток кабелей и других токопроводящих коммуникаций с нулевым потенциалом Земли.

Закладное устройство [secret intelligence device] — скрытно устанавливаемое техническое средство осуществления угрозы информации.

Законный (правильный) [legitimate] — соответствующий принятым законам, нормативной базе.

Законодательство о защите данных [Data protection legislation] — законодательство, принятое или принимаемое во всех странах для защиты персональных данных, обрабатываемых компьютерами. Цель законодательства заключается в контроле и предотвращении неправильного использования информации в случае, когда персональные данные хранятся в компьютере.

Закрытая информация [Private information] — информация, которая по тем или иным соображениям представляет тайну и распространение которой возможно лишь с согласия органов, уполномоченных контролировать вопросы, связанные е этой информацией.

Закрытые (защищенные) данные [Resticted data] — данные, доступные ограниченному кругу пользователей. Как правило, ограничение доступа достигает системой паролей.

Замок защиты (секретности) [Memory lock] — программный механизм проверки паролей при обращении к базе данных или ее фрагментам (файлам, областям), обеспечивающий ограничение доступа к записям.

Замок памяти [Memory lock] — код в дескрипторе сегмента или страницы виртуальной памяти, используемый системой защиты памяти для ограничения доступа. При этом к сегменту могут обращаться только процессы, имеющие в своем дескрипторе соответствующий ключ.

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

Запрос идентификации (опознания) [Interrogation] — запрос, заданный ведущей станцией ведомой станции для ее идентификации или определения ее состояния.

Заражение [Infection] — в вычислительной технике процесс создания вирусом своей копии, связанный с изменением кодов программ, системных областей или системных таблиц.

Зарегистрированный пользователь [Authorized user] — 1) Пользователь, имеющий приоритетный номер в

данной системе коллективного пользования. 2) Пользователь, включенный в график работ на ЭВМ.

Зашифрованные данные [Cipher data] — информация, хранящаяся в памяти ЭВМ в зашифрованном виде, т.е. данные, к которым применен способ криптографической защиты.

Зашифрованный текст [Ciphertext] — результат зашифрования исходного открытого текста, осуществляемого с целью сокрытия его смысла.

еще — зашифрованная форма сообщений или данных.

Защита [Protection, security, lock out] — средство для ограничения доступа или использования всей или части вычислительной системы; юридические, организационные и технические, в том числе программные, меры предотвращения несанкционированного доступа к аппаратуре, программам и данным.

Защита выделенного помещения — проведение комплекса организационно — технических мероприятий по предотвращению утечки речевой секретной или конфиденциальной информации по техническим каналам за пределы выделенного помещения. В общем случае комплекс мероприятий по защите выделенных помещений включает: защиту речевой информации, обрабатываемой техническими средствами от утечки за счет электромагнитных излучений и наводок (ПЭМИН); защиту речевой информации от утечки за счет эффекта электроакустического преобразования вспомогательных технических средств и систем (ВТСС); защиту речевой информации от утечки за счет лазерного зондирования стекол или стетоскопического прослушивания ограждающих конструкций; защиту речевой информации от утечки за счет несанкционированного доступа в помещение и скрытой установки в нем подслушивающих приборов (микрофонов, магнитофонов, радиопередатчиков и т.д.); акустическую защиту помещений.

Защита вычислительной сети [Network security] — исключение несанкционированного доступа пользователей к элементам и ресурсам сети путем использования аппаратных, программных и криптографических методов и средств защиты, а также организационных мероприятий.

Защита границ [Boundary protection] — использование ограничительных регистров (регистров защиты памяти) для защиты ресурсов компьютера.

Защита данных [data protection] — охрана данных от несанкционированного, умышленного или случайного их раскрытия, модификации или уничтожения (ДСТУ 2874).

Защита информации — включает в себя комплекс мероприятий, направленных на обеспечение информационной безопасности. На практике под этим понимается поддержание целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных. [11]

еще — деятельность, направленная на сохранение государственной, служебной, коммерческой или личной тайн, а также на сохранение носителей информации любого содержания. Существуют три основные формы защиты информации: правовая, организационно-техническая и страховая.

еще — использование в системах сбора, передачи, хранения и переработки информации специальных методов и средств в целях обеспечения сохранности защищаемой информации и предотвращения ее утечки по техническим каналам.

Защита информации от технических разведок — деятельность, направленная на предотвращение или существенное снижение возможностей технических разведок по получению разведывательной информации путем разработки и реализации системы защиты. Замысел защиты информации от технических разведок должен удовлетворять требованиям (принципам) комплексности, активности, убедительности, непрерывности и разнообразия.

Защита информации при ее обработке техническими средствами — действия, направленные на обеспечение безопасности информации при ее обработке техническими средствами от всех видов угроз и факторов опасности. При обработке информации техническими средствами различают организационную и техническую защиты.

Защита накоплением — метод восстановления данных, хранящихся во внешней памяти, состоящий в том, что на дополнительный носитель копируются только те файлы, которые были созданы позднее определенного срока.

Защита объектов [Object protection] — средства защиты объектов типа сейфов, файлов и т.д.

Защита от записи [Writeprotect] — способ защиты информации на диске и/или в оперативной памяти, заключающийся в установке ключей защиты или в заклеивании метки считывания на диске, что предотвращает запись новых данных и сохраняет имеющиеся от разрушения.

Защита от копирования [Copyprotection] – программно-аппаратное средство для предотвращения копирования некоторой записанной информации в другую часть памяти или на другое запоминающее устройство. Диск с защищенной информацией не может быть скопирован стандартными средствами.

Защита от несанкционированного доступа [Protection from unauthorized access] — предотвращение или существенное затруднение несанкционированного доступа к программам и данным путем использования аппаратных, программных и криптографических методов и средств защиты, а также проведение организационных мероприятий. Наиболее распространенным программным методом защиты является система паролей.

Защита от несанкционированной выборки [Fetch protect] — ограничение возможности считывания из определенного сегмента ЗУ.

Защита от ошибок [Error protection] — 1) Применение кодов с обнаружением и исправлением ошибок. 2) Действия по проверке правильности выполнения предыдущих операций. 3) Контроль допустимости значений аргументов при входе в процедуру.

Защита памяти [Memory protection] — один из многих способов управления доступом или использования памяти. Это управление может предотвратить некорректное вмешательство пользователя, обеспечить защиту системы или выполнять сразу обе эти функции. Механизм контроля за доступом к какойлибо области памяти с учетом разработанных обращений известен как защита памяти. Разрешенный режим обращения может быть различным для разных процессов. При разметке области оперативной памяти могут использоваться граничные регистры; конкретные зафиксированные участки памяти могут контролироваться с помощью блокировочных замков; доступ к конкретным словам может контролироваться посредством тегов.

Защита паролем (с помощью пароля) [Password protection] – способ защиты данных, при котором для получения доступа к ним необходимо ввести пароль.

Защита по записи [Write protection] — запрещение обращения к файлу для выполнения операции записи данных. Разрешается только чтение данных.

Защита по чтению [Read protection] — запрещение обращения к файлу для выполнения операции чтения данных. Разрешается только запись данных.

Защита прав пользователей — совокупность правил, методов и средств, направленных на обеспечение беспрепятственного и своевременного доступа пользователей к программам и данным и защиту их информации от использования другими лицами.

Защита программы [Software lock] — свокупность условий, предотвращающих запуск программы на выполнение.

Защита системы [System security] — совокупность мер, предпринимаемых для исключения несанкционированного доступа к программам и данным системы или случайного вмешательства в ее работу.

Защита собственности [Privacy protection] — совокупность технических, административных и физических мер, реализованных с целью обеспечения безопасности и конфиденциальности записей данных, равно как и для защиты подсистем безопасности и конфиденциальности от любых случайных или преднамеренных действий, которые могут привести к затруднению, ущербу, неудобствам или несправедливости в отношении лица, о котором хранится соответствующая информация.

Защитное сооружение — специальное сооружение (конструкция), предназначенное для защиты объекта от технических разведок.

Защищенная ИС — ИС, в которой реализованы механизмы выполнения правил, удовлетворяющих установленному на основе анализа угроз перечню требований по защите информации и компонентов этой ИС. При этом механизмы выполнения указанных правил чаще всего реализуются в виде *системы защиты информации*.

Защищенная область [Protected area] — в базах данных область, доступ к которой требует ввода пароля.

Защищенная обработка [Protected processing] — режим обработки области базы данных, при котором все остальные одновременно выполняемые процессы могут только читать, но не могут изменять (обновлять, добавлять, удалять) записи этой области.

Защищенная программа [Copyprotected software] — программа, защищенная от копирования.

Защищенная система [Protected system] — система, вход в которую требует ввода пароля.

Защищенное техническое средство обработки информации — техническое средство обработки информации, в котором средства и способы защиты реализованы на стадиях его разработки и изготовления.

Защищенность — в вычислительной технике способность системы противостоять несанкционированному доступу к программам и данным (безопасность,

секретность), а также их случайному искажению или разрушению (целостность).

Защищенные средства [protected facilities] — основные и вспомогательные технические средства, в которых предусмотрено предотвращение осуществления угроз информации.

Защищенные средства вычислительной техники (защищенные автоматизированные системы) [Trusted computer system] — средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты.

Защищенный объект информатики — объект информатики, соответствующий требованиям стандартов и других нормативных документов по обеспечению безо пасности обрабатываемой информации.

Защищенный режим использования [Protected usage mode] — режим, защищенной обработки базы данных, в котором все прикладные программы, работающие параллельно с программой, открывшей области базы данных в этом режиме, могут читать записи, но не могут их обновлять до тех пор, пока программа не закроет эти области.

Защищенный ресурс [Locked resource] — ресурс, для которого определен замок секретности, т.е. специфицировано управление доступом.

Защищенный файл [Protected file] — файл, для доступа к записям которого необходимо ввести пароль.

Злоумышленник [Intruder] — лицо или организация, заинтересованные в получении несанкционированного доступа к программам или данным, предпринимающие попытку такого доступа или совершившие его.

Злоумышленное использование вычислительной машины [Computer fraud] — любая деятельность, направленная на манипулирование информацией внутри вычислительной системы с целью личной выгоды, обычно финансовой.

Знак соответствия в области защиты информации — защищенный в установленном порядке знак, применяемый или выданный в соответствии с правилами системы сертификации, указывающий, что обеспечивается необходимая уверенность в том, что данное защищенное изделие,техническое средство или способ защиты информации соответствует конкретному стандарту или другому нормативному документу.

Зона безопасности [safety zone] — Пространство, в пределах которого обеспечивается требуемый уровень защиты информации.

Зона разведдоступности — часть пространства вокруг объекта, в пределах которого реализуются возможности технической разведки.

Зона электромагнитного зашумления — пространство вокруг устройства электромагнитного зашумления, в пределах которого уровень создаваемых маскирующих помех выше уровня электромагнитного фона (уровня стабильных индустриальных помех).

И

Идентификатор [Identifier] — средство идентификации доступа, представляющее собой отличительный признак субъекта или объекта доступа. Основным средством идентификации доступа для пользователей является пароль.

еще — лексическая единица, используемая в качестве имени для элементов языка; имя, присваиваемое данному и представляющее собой последовательность латинских букв и цифр, начинающуюся с буквы.

Идентификатор диагностического сообщения — код сообщения, выдаваемого системной программой в ответ на обнаруженную ошибку.

Идентификатор доступа [Access identifier] — уникальный признак субъекта или объекта доступа.

Идентификатор задачи [Task identifier] — символьный код, приписы ваемый выполняющейся или готовой к выполнению задаче.

Идентификатор пользователя [User identifier, userid] — символи ческое имя, присваиваемое отдельному лицу или группе лиц и разрешающее использование ресурсов вычислительной системы.

еще — опознавание пользователя (по фамилии их паролю) для определения его полномочий и прав на доступ к данным и выбора режима их использования.

Идентификационная (кодовая) карта — перфорированная бумажная или магнитная карта с нанесенным на ней кодовым словом (паролем), предназначенная для идентификации доступа пользователя к информационному ресурсу.

Идентификация [Identification] — присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

еще — процесс распознавания определенных компонентов системы, обычно с помощью уникальных, воспринимаемых системой имен (идентификаторов).

Иерархическая модель данных [hierarchical model] — модель данных для представления данных иерархической структуры (ДСТУ 2874).

Иерархическая структура данных [hierarchical data structure] — структура данных, представляющая собой множество, частично упорядоченное таким образом, что существует только один элемент этого множества, не имеющий предыдущего, а все другие элементы имеют только один предыдущий (ДСТУ 2874).

Избирательное управление доступом [Discretionary access control (DAC)] — метод управления доступом субъектов системы к. объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит. Управление является избирательным в том смысле, что субъект с определенными правами может осуществлять передачу прав любому объекту независимо от установленных ограничений (доступ может быть осуществлен и не напрямую).

Избыточная система [Redundant system] — система, обладающая избыточностью некоторого типа аппаратной, алгоритмической, информационной, обеспечивающей повышение надежности ее функционирования.

Избыточность [Redudancy] — введение в систему дополнительных компонентов сверх минимально необходимого их числа с целью повышения надежности системы. Различают избыточность аппаратную, информационную, алгоритмическую.

Избыточность кода (кодовая избыточность) [Code redudancy] — разность между средним числом битов, используемых для кодирования одного сообщения источника и минимально возможным числом битов, полученным из теоремы Шеннона.

Изменение формата [Format altration] — использование нестандартного формата диска для защиты от копирования; в этом случае диск не может быть прочитан стандартными утилитами копирования.

Изменяющийся во времени код [Timevariant code] — код, слова которого некоторым образом изменяются в процессе работы. См. также случайный код.

Изолирующая вставка — развязывающее приспособление, представляющее собой токонепроводящую вставку в токопроводящих коммуникациях (например, отрезок керамической трубы в металлическом трубопроводе).

Имитация — составная часть технической дезинформации, осуществляемая путем искусственного воспроизведения ложных объектов и технических демаскирующих признаков.

Имитация экрана [Screen mimic] — маскировка экрана, обычно связана с высвечиванием ничего не подозревающему пользователю ложного экрана опроса для перехвата его имени и пароля.

Имитовставка — отрезок информации фиксированной длины, полученный по определенному правилу из открытых данных и ключа и добавленный к зашифрованным данным для обеспечения имитозащиты.

Имитозащита — защита системы шифрованной связи от навязывания ложных данных.

Индивидуальный учет [Individual accountability] — комплекс мер, за счет которых идентификация пользователя может быть использована для определения возможности доступа пользователя к машинам, материалам и т.п.; правила предоставления пользователю времени, методов и режимов доступа.

Инициализация [Initialization] — установка электрических цепей или программных сред в начальное состояние обычно при первом включении; возможно выполнение того же действия и в дальнейшем по инициативе оператора.

Инсталляция [Installation] — 1) Установка программного изделия на ПЭВМ. 2) Одно из ограничений на программное изделие при продаже его фирмой.

Интенсивность акустических колебаний — колебательная мощность, действующая на единице площади фронта волны $I = P \cdot V = P^2/Zb = V^2 \cdot Zb$, где I — интенсивность колебаний, вт/м^2; P — акустическое давление, н/м^2; V — колебательная скорость, м/с; Zb — волновое сопротивление среды, н.с/м^2.

Интерпретация [interpretation] — анализ команд или операторов программы и немедленное их выполнение (ДСТУ 2873).

Интерфейс (в системах обработки данных) [interface (in data pro cessing systems)] — определенный набор услуг, представляемых процессором (ДСТУ 2874).

Информативность побочных электромагнитных излучений и новодок — наличие в составе побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации, признаков обрабатываемой информации.

Информативный сигнал [informative signal] — физический сигнал или химическая среда, содержащие информацию с ограниченным доступом.

Информатизация — организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.

Информационная акустика — научное направление, связанное с разработкой моделей акустических исследований, обработкой акустических сигналов и передачей акустической информации в упругих средах различной физической природы.

Информационная безопасность — это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры [11].

Информационная дивергенция [Informational divergence] — функция, определенная для двух распределений вероятностей и характеризующая степень их близости. Широко используется в задачах теории информации.

Информационная надежность [Information reliability] — 1) Способность алгоритма или программы правильно выполнять свои функции при различных ошибках в исходных данных. 2) Способность информационной системы обеспечивать целостность хранящихся в ней данных.

Информационная система — организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Информационная система [information system] — система, организующая память и манипулирование информацией о проблемной области (ДСТУ 2874).

Информационная технология — система технических средств и способов обработки информации.

Информационные процессы — процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Информационные ресурсы — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). *Информационные ресурсы* могут быть государственными и негосударственными и как элемент состава имущества находятся в собственности граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений. Отношения по поводу права собственности на информационные ресурсы регулируются соответствующим гражданским законодательством.

Информационный барьер [Information barrier] — Совокупность различных препятствий, возникающих на пути распространения и использования информации.

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

еще — сведения, раскрываемые технической разведкой через демаскирующие признаки объектов защиты или путем несанкционированного доступа к техническим средствам обработки информации.

еще — совокупность данных, обрабатываемых технических средствами.

еще — совокупность сведений об объектах и явлениях материального мира, рассматриваемых в аспекте их передачи в пространстве и времени. Информация передается в виде сообщений с помощью сигналов.

еще — совокупность сведений, связанных с изменением состояния материальных объектов и восприятием этих изменений другими объектами методом отражения. Информация рассматривается также как количественная мера изменений состояния материальных объектов. Как философская категория информация имеет содержание и формы своего существования (проявления).

Информация (для процесса обработки данных) [information (in data processing)] — любые знания о предметах, фактах, понятиях и т.д. проблемной области, которыми обмениваются пользователи системы обработки данных (ДСТУ 2874).

Информация аутентификации [Authenfication information] — информация, используемая для установления подлинности личности, за которую выдает себя пользователь.

Информация о гражданах (персональные данные) — сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

Информация с ограниченным доступом [limited access information] — информация, право доступа к которой ограничено установленными юридическими нормами и правилами

Искажение [Distortion] — отклонение значений параметров сигнала данных от установленных требований.

еще — изменение содержимого сообщения, передаваемого по линии связи.

Искажение информации — случайная несанкционированная модификация информации при ее обработке техническими средствами в результате внешних воздействий (помех), сбоев в работе аппаратуры или неумелых действий обслуживающего персонала.

Исправление [Correction] — внесение изменений в программу или набор данных путем обновления, добавления или удаления отдельных частей (фрагментов).

Испытание (тестирование, проверка) [Test, testing] — проверка системы или ее компонента путем реального выполнения какихлибо задач.

Испытание на проникновение [Penetration test] — испытание системы с целью проверки средств ее защиты (в частности от несанкционированно го доступа).

Испытательная модель [Test bed] — любая система, основным назначением которой является обеспечение основы для тестирования других систем. Испытательные модели обычно делаются под определенный язык программирования и методы реализации, а часто и под определенные прикладные задачи.

Источник — материальный объект или субъект, информации способный накапливать, хранить, преобразовывать и выдавать информацию в виде сообщений или сигналов различной физической природы.

Исчерпывающий поиск [Exhaustive search] — поиск данных методом перебора. Является идеальным по критериям полноты и точности, но малоэффективным по временным показателям для больших информационных каналов.

K

Канал [Channel] — часть коммуникационной системы, связывающая между собой источник и приемник сообщений.

Канал утечки акустической (речевой) информации — совокупность источника акустических колебаний (источника речевой информации), среды распространения акустических сигналов и акустического приемника, обусловливающая возможность обнаружения и перехвата акустической (речевой) информации. В общем случае средой распространения акустических колебаний могут быть газовые (воздушные) , жидкостные (водные) и твердые среды, в том числе недра Земли.

Канал утечки информации [Covert channel] — канал коммуникации, позволяющий процессу передавать информацию путем, нарушающим безопасность системы.

Канальное кодирование (1) [Channel coding] — использование кодов с обнаружением ошибок или кодов с исправлением ошибок для обеспечения надежной передачи по каналу связи. При канальном кодировании код выбирается в соответствии с каналом (главным образом, с его шумовыми характеристиками), а не с источником информации.

Канальное кодирование (2) [Link encruption] — способ передачи за шифрованных сообщений, при котором каждое сообщение дешифрируется и перекодируется вновь после каждого этапа его пересылки.

Канальное шифрование [Link encryption] — защита информации, передаваемой средствами телекоммуникаций криптографическими методами; шифрование осуществляется в канале связи между двумя узлами (которые могут быть промежуточными на пути от отправителя к получателю).

еще — реальное применение процедур шифрования данных в каждом канале передачи данных коммуникационной системы.

Карта копирования [Copy card] — электронное устройство, которое, будучи включенным в компьютер, позволяет копировать защищенное программное обеспечение из оперативной памяти на диск.

Карта с микропроцессором [Chip card] — пластмассовая карточка типа кредитной, но имеющая встроенные ЗУ и микропроцессор (или специализированную логическую схему).

Каскадный код [Factorable code] — код с исправлением ошибок, который можно рассматривать как результат последовательного применения нескольких других кодов.

Категория [Category] — класс, уровень категоризации.

Категория безопасности информации — уровень безопасности информации, определяемый установленными нормами в зависимости от важности (ценности) информации.

Категория допуска (уровень защиты) [Security clearance] — категоризация информации, связанная с субъектом, например с пользователем, и проводимая для выполнения категории защиты той информации, к которой этому пользователю предоставлено право доступа.

Категория защиты [Security classification] — классификация доступности информации, например, "секретная информация" или "медицинская информация только для врачей".

Категория защиты информации — качественный показатель, отражающий степень важности защиты информации в выбранной шкале ценностей.

Категория управления доступом [Access control category] — языковые элементы, предназначенные для определения правил, предохраняющих от несанкционированных операций.

Качество [Quality] — совокупность свойств изделия, обуславливающих его пригодность удовлетворять определенные потребности в соответствии с его предназначениями. Качество определяется показателями качества такими, как надежность, точность, полнота, быстродействие и т. п.

Качество данных [Quality of data] — совокупность свойств данных, обеспечивающих их пригодность для решения определенных задач. К пока зателям качества данных относятся: точность, полнота, адекватность, непротиворечивость, защищенность и др.

Качество документации [Documentation quality] — характеристика программной документации, определяемая полнотой и точностью описания программного изделия, наглядностью и удобочитаемостью материала, что позволяет быстро осваивать и эффективно использовать это изделие.

Класс защищенности средств вычислительной техники (автоматизированной системы) [Protection class of computer system] — определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации.

Класс идентификатора [Naming class] — категория, определяющая способ связи идентификатора со значением и способ его использования.

Классификации угроз среде ИС:

- Неавторизованная модификация данных и программ — происходящая в результате модификации, удаления или разрушения человеком данных и программного обеспечения ИС неавторизованным или случайным образом.
- Неавторизованный доступ к ИС — происходящий в результате получения неавторизованным человеком доступа к ИС.
- Неработоспособность ИС — происходящая в результате реализации угроз, которые не позволяют ресурсам ИС быть своевременно доступными.
- Несоответствующий доступ к ресурсам ИС — происходящий в результате получения доступа к ресурсам ИС авторизованным или неавторизованным человеком неавторизованным способом.
- Подмена трафика ИС — происходящая в результате появлений сообщений, которые имеют такой вид, как будто они посланы законным заявленным отправителем, а на самом деле сообщения посланы не им.
- Раскрытие данных — происходящее в результате получения доступа к информации или ее чтения человеком и возможного раскрытия им информации случайным или неавторизованным намеренным образом.
- Раскрытие трафика ИС — происходящее в результате получения доступа к информации и возможного ее разглашения случайным или неавторизованным намеренным образом тогда, когда информация передается через ИС.

Ключ (шифрования) — конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования информации, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

Ключ [Key] — совокупность знаков, используемая для идентификации записей в файле и быстрого доступа к ней.

еще — код, используемый для подтверждения полномочий на доступ к некоторой информации (см.пароль).

еще — значение, на основе которого производится шифрование.

еще — идентификатор, содержащийся внутри набора элементов данных (ДСТУ 2874).

Ключ базы данных [database key] — Ключ, присвоенный системой управления базами данных и однозначно идентифицирующий запись базы данных (ДСТУ 2874).

Ключ защиты памяти [Protection key] — код, присваиваемый блоку памяти, выделенному программе, и используемый для обращения программы к памяти в целях ее защиты. Должен совпадать с ключом защиты; при несовпадении задание завершается аварийно.

Ключ секретности [Privacy key] — ключ, значение которого система использует для определения того, должен ли защищенный ресурс быть доступным процессу, выдавшему данное значение ключа.

Ключ управления доступом [Access control key] — значение, предъявляемое процессом системе управления базами данных и сравниваемое ею с соответствующим замком с целью предотвращения несанкционированного доступа к данным.

Ключевая система [Key management] — совокупность криптографических ключей и правил обращения с ними при обеспечении криптографической защиты информации.

Код [Code] — 1) Представление символа двоичным кодом. 2) Криптографический прием, в котором используется произвольная таблица или кодировочная книга для преобразования текста в закодированную форму.

Код с контролем на четность [Paritychek code] — двоичный код, в котором к каждой кодовой комбинации присоединяется дополнительный контрольный разряд, что позволяет сохранить принятую в системе одну и ту же четность двоичных блоков.

Код с минимальной избыточностью [Minimumredudancy code] — как правило, под этим подразумевается код, построенный по процедуре Хаффмана; в общем случае "оптимальный" код с точки зрения средней длины кодового слова, сложность реализации кодирования не рассматривается.

Код с минимальным расстоянием [Minimumdistance code] — избыточный код, в котором переход от одного допустимого значения к следующему сопровождается минимальным изменением в кодовой комбинации. Позволяет обнаруживать в передаваемых данных только одиночные ошибки.

Код с обнаружением ошибок [Errorchecking (erroedetecting, selfchecking) code] — см. двоичный код с обнаружением ошибок.

Код с переменной скоростью [Ratevariant code] — как правило, используется при описании сверточных кодов, у которых длина кодовых подблоков изменяется во времени, а длина информационных подблоков остается постоянной.

Код Хаффмана [Huffman code] — Префиксный код, в котором длина кодовой комбинации обратно пропорциональна частоте появления кодируемого элемента (чем чаще встречается элемент, тем короче кодовая комбинация).

Код Хемминга [Hamming code] — код с минимальной избыточностью, обеспечивающий исправление одиночных ошибок.

Кодирование [Coding, encoding] — 1) Отождествление данных с их кодовыми комбинациями; установление соответствия между элементом данных и совокупностью символов, называемой кодовой комбинацией, словом кода. 2) Преобразование детальной спецификации в программу.

Кодирование источника (или сжатое кодирование) [Souurce coding (comparison coding)] — использование в рамках заданного алфавита кодов переменной длины с целью уменьшения числа символов в сообщении до минимума, необходимого для представления всей информации сообщения или по крайней мере для обеспечения условий такого сокращения. При кодировании источника конкретный код выбирается на основе характеристик источника сообщения (т.е. относительных вероятностей появления различных знаков алфавита в исходной программе), а не на основе характеристик канала, по которому в конечном счете будет передаваться сообщение.

Кодирование с критерием верности [Coding with fidely criterion] — преобразование сообщения источника в кодовое слово, такое, что обратное преобразование приводит к некоторому другому сообщению, близкому к исходному в смысле заданного критерия верности.

Кодирование, использующее флаг [Flag encoding] — к коду добавляется некоторая последовательность символов, которая не является кодовым словом и в процессе работы может быть использована как разделитель между словами.

Кодирующее устройство [Coder] — 1) Автоматическое или автоматизированное устройство для кодирования программ и данных на носителе информации с целью последующего их ввода в ЭВМ. 2) Устройство для преобразования вида представления информации, в котором каждому входному сигналу соответ-

ствует определенная комбинация выходных сигналов, являющихся кодом входного сигнала.

Кодовая решетка [Code trellis] — направленный граф, в который превращается дерево сверточного кода с конечной длиной ограничения.

Коды Боуза Чоудхури Хокенгема (коды БЧХ) [Bose Chaudhuri Hocquenghem codes (BCH codes)] — семейство двоичных линейных блоковых кодов с исправлением ошибок. Эти коды весьма эффективны, но главное их преимущество состоит в простоте кодирования/декодирования (с использованием сдвиговых регистров). Их можно рассматривать и как обобщение кодов Хэмминга, и как специальный случай кодов РидаСоломона. Коды БЧХ используются и в качестве циклических кодов.

Коды Голея [Golay codes] — семейство совершенных линейных блоковых кодов с исправлением ошибок. Наиболее полезным является двоичный код Голея. Известен также троичный код Голея. Коды Голея можно рассматривать как циклические коды.

Коды Рида Мюллера [ReedMuller codes (RM codes)] — семейство двоичных циклических блоковых кодов с исправлением ошибок.

Коды Рида Соломона [ReedSolomon codes (RS codes)] — важное семейство линейных блоковых кодов с исправлением ошибок, особенно удобных для исправления пакетов ошибок. Они могут рассматриваться и как обобщение кодов БоузаЧоудхуриХокенгема, и как особый случай кодов Гоппы, могут быть отнесены к циклическим кодам.

Коды с повторением [Repetition codes] — семейство совершенных циклических блоковых кодов с исправлением ошибок, в котором ключевые слова формируются просто r-кратным повторением слов сообщения. Если данные коды рассматривать как коды с параметрами (n,k), то для любого k у них $n = rk$.

Коллективный (групповой) доступ [Shared access] — совместное использование вычислительной системы двумя или более пользователями в пакетном или интерактивном режимах.

Комбинаторный источник информации [Combinatorial source] — источник, на выходе которого может появиться одна из последовательностей, принадлежащая заданному конечному множеству (например, множество векторов фиксированного веса Хемминга).

Комбинированный взрыв [Combination blowup] — в интеллектуальных системах ситуация, когда размер пространства решений увеличивается чрезвычайно быстро с ростом числа элементарных решений. По этой причине метод перебора для поиска решения становиться неприемлемым: необходимо использовать эвристические правила.

Коммерческая информация [Commercial information] — информация, распространяемая только по желанию ее обладателя и на его условиях; объект купли-продажи.

Коммерческая тайна — сведения конфиденциального характера из любой сферы деятельности государственного или частного предприятия, разглашение которых может нанести материальный или моральный ущерб ее владельцам или пользователям (юридическим лицам). Охрана коммерческой тайны осуществляется ее владельцем.

Коммуникационный барьер [Communication barrier] — барьер, возникающий в процессе взаимодействия между системными аналитиками и управленческим персоналом предприятия (учреждения) при разработке и внедрении автоматизированных систем.

Компилятор [compiler] — транслятор, предназначенный для выполнения компиляции (ДСТУ 2873).

Комплекс средств защиты [Trusted computing base] — совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации.

Комплексность защиты — принцип защиты, предусматривающий мероприятия против всех опасных видов и средств технической разведки.

Компрометация [Compromise] — Утеря критичной информации либо получение ее неавторизованными для этого субъектами (лицами, программами, процессами и т.д.)

Компьютерное преступление — осуществление несанкционированного доступа к информационному ресурсу, его модификация (подделка) или уничтожение с целью получения имущественных выгод для себя или для третьего лица, а также для нанесения имущественного ущерба своему конкуренту.

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

Контролируемая зона — территория вокруг технического средства обработки информации, в пределах которой не допускается несанкционированное пребывание посторонних лиц и транспортных средств. Размер контролируемой зоны должен быть не менее размера зоны 2.

Контролируемая территория [controllable territory] — пространство или территория, в пределах которых исключено неконтролируемое пребывание посторонних лиц контроль [Check] — Совокупность действий, позволяющих получать независимый обзор и анализ системных записей и активности системы с целью установления ее текущего состояния безопасности.

Контроль данных [Data check] — проверка достоверности и целостности данных. Различают синтаксический, семантический и прагматический контроль.

Контроль доступа [Access control] — определение и ограничение доступа пользователей, программ или процессов к устройствам, программам и данным вычислительной системы.

Контроль дублированием [Duplication check] — контроль двух тождественных процессов посредством сравнения их результатов. Полное совпадение результатов свидетельствует об отсутствии ошибок.

Контроль качества [Quality control] — использование методов выборки, проверки и испытания на всех уровнях разработки системы с целью выпуска бездефектного оборудования и программного обеспечения.

Контроль на основе избыточного циклического кода [Cyclic redundancy chek (CRC)] — способ продольного контроля данных, который обеспечивает коррекцию ошибок.

Контроль по избыточности [Redundacy check] — контроль, выполняемый или с помощью резервированных технических средств, или на основе избыточной информации и обеспечивающий выдачу сведений о наличии определенных ошибок.

Контроль по модулю *n* (контроль по остатку) [Checksum, modulon check, residue check] — простой метод обнаружения ошибок, основанный на анализе некоторого набора данных или участка программы. Если этот набор представляет собой совокупность блоков длиной *m* бит, то берется сумма по модулю *n*, где $n = 2^{**}m$, и ставится в конец набора. Позднее (например, после пересылки набора данных в другое место) можно осуществить повторное вычисление контрольной суммы; при этом будут выявлены одиночные ошибки на уровне битов. Простейшим вариантом метода ($m = 1$, $n = 2$) является контроль четности.

Контроль правильности (проверка достоверности) [Validity check] — любая проверка соответствия некоторого объекта установленным ограничениям. Например, если какое-либо значение элемента данных вводится программой, то обычно этой программой осуществляется проверка значения на соответствие заданному диапазону.

Контроль работы с данными [Manipulation detection] — процедура, позволяющая выявить, подвергался ли блок данных случайным или преднамеренным воздействиям.

Контроль средств защиты [Security audit] — инспекция системных записей и работы персонала с целью проверки функционирования систем защиты, их соответствия принятой стратегии требованиям эксплуатации, а также выработки соответствующих рекомендаций.

Контроль четности [Parity check] — метод контроля данных, при котором сумма по модулю 2 двоичных единиц в машинном слове, включая контрольный разряд, должна иметь определенное значение: быть всегда четной или нечетной. Неравенство суммы этому значению говорит об ошибке в данных.

Контроль эффективности защиты информации — проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты.

Контрольная запись [Control record] — запись, которая содержит контрольные суммы, вычисленные путем суммирования значений из других записей файла. Контрольные суммы могут нести дополнительную информацию или использоваться только для проверки правильности данных.

Контрольная сумма [Control (hash) total, checksum] — информация, предназначенная для проверки правильности записи данных путем подсчета суммы байтов и добавления ее к записи; при считывании данных сумма байтов должна совпасть с контрольной суммой.

Контрольный журнал [Audit trail] — журнал, в котором фиксируются обращения к защищенным данным. Просмотр этого журнала позволяет выявить попытки несанкционированного доступа и идентифицировать лиц, делавших такие попытки.

Контрольный код [Check code] — код, позволяющий автоматически обнаруживать, локализовывать и устранять ошибки в передаваемых данных.

Конфиденциальная информация — информация, которая представляет собой коммерческую или личную тайны и охраняется ее владельцем.

Конфиденциальная информация [Sensitive information] — информация, требующая защиты.

Конфиденциальность [Confidentiality] — 1) Некоторый класс данных, получение либо использование которых неавторизованными для этого лица ми может стать причиной серьезного ущерба для организации. 2) Свойство информации, состоящее в том, что она не может быть обнаружена и сделана доступной без разрешения отдельным лицам, модулям или процессам.

еще — содержание критичной информации в секрете, доступ к ней ограничен узким кругом пользователей (отдельных лиц или организаций).

Конфиденциальность потока сообщений (К. трафика) [Traffic flow confidentiality] — услуги конфиденциальности, обеспечивающие защиту от анализа потока сообщений, трафика.

Концептуальная модель [conceptual model] — формальное представление проблемной области на понятийном уровне (ДСТУ 2874).

Концепция диспетчера доступа [Reference monitor concept] — концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях субъектов к объектам.

Концепция доступа — модель управления доступом, осуществляемая в абстрактной ЭВМ, которая посредничает при всех обращениях субъектов к информационным ресурсам. Существуют следующие концепции доступа : дискреционное управление, мандатное управление, многоуровневая защита.

Концепция защиты информации — система взглядов и общих технических требований по защите информации.

Концепция монитора ссылок [Reference monitor concept] — концепция контроля доступа, базирующаяся на понятии абстрактной машины, разделяющей все попытки доступа субъектов к объектам. Находит практическую реализацию в виде ядра безопасности.

Коррелированные источники [Correlated sources] — источники, порождающие статистически зависимые последовательности символов.

Косвенный демаскирующий признак объекта — технический демаскирующий признак, обусловленный действием обеспечивающих сил и средств или изменением окружающей среды в результате функционирования объекта защиты. К косвенным демаскирующим признакам относятся визуально-оптические признаки деятельности объекта, а также химическое или радиоактивное заражение местности.

Коэффициент сжатия в источнике сообщений [Source compressing factor] — отношение длин сообщения до и после его сжатого кодирования.

Коэффициент экранирования технического средства обработки информации — степень ослабления воздействия внешних электромагнитных излучений на электронные элементы технического средства обработки информации через электромагнитное поле за счет соответствующего выбора базовых несущих конструкций и применения других аппаратных способов защиты.

еще — степень ослабления воздействия внешних электромагнитных излучений на электронные элементы технического средства обработки информации через проводящие коммуникации, гальванически подключаемые к техническому средству. Основным средством электромагнитной рвазвязки являются электрические помехозащитные фильтры различного назначения. Для устранения внешнего электромагнитного влияния по цепям электроснабжения используются мотор — генераторы и устройства гарантированного питания (УГП), первичным источником электропитания которых являются аккумуляторы.

Кратковременная ошибка [Soft error] — ошибка изза случайных обстоятельств, сбой.

Криптоанализ [Criptoanalysis] — изучение системы защиты сообщений и/или исследование ее входных и выходных сообщений с целью выделить скрытые переменные или истинные данные, включая исходный текст.

Криптографическая защита [Cryptosecurity (criptographical security)] — защита информации путем осуществления ее криптографического преобразования.

Криптографическая проверка [Cryptographic checkvalue] — процесс извлечения информации с помощью криптографического преобразования.

Криптографическая система [Cryptosystem] — совокупность технических и/или программных средств, организационных методов, обеспечивающих крип-

тографическое преобразование информации и управление процессом распределения ключей.

Криптографический ключ [Cryptology key] — последовательность символов, обеспечивающая возможность шифрования и дешифрования.

Криптографический метод защиты информации — метод защиты информации, основанный на принципе ее шифрования. Криптографический метод может быть реализован как программными, так и аппаратными средствами.

Криптографическое преобразование (информации) — преобразование информации при помощи шифрования и/или выработки имитовставки.

Криптография [Cryptography] — принципы, средства и методы преобразования информации к непонятному виду, а также восстановления информации к виду, пригодному для восприятия.

еще — область знаний, которая объединяет принципы, методы и средства преобразования данных с целью замаскировать содержание информации, предотвратить возможность ее перехвата и искажения информации, защитить от несанкционированного доступа к информации.

Криптопреобразования (криптографические преобразования) [Cryptographical transformation] — совокупность операций шифрования и дешифрования данных, а также перешифрования данных при смене шифра.

Критерий безопасности информации — показатель, характеризующий безопасность информации при воздействии различных факторов опасности. Критериями безопасности могут быть следующие показатели: для ПЭМИН — абсолютный уровень ПЭМИН или соотношение информационный сигнал/помеха в эфире и токопроводящих коммуникациях; для НСД — вероятность НСД; для аппаратных закладок — наличие проведенной спецпроверки по поиску и аннулированию закладных устройств; для внешних воздействий на информационный ресурс — вибростойкость, влагостойкость, пожаростойкость, устойчивость против электромагнитного воздействия.

Критичная информация [sensitive information] — любая информация, потеря, неправильное использование, модификация или раскрытие которой могут нанести ущерб национальным интересам, или помешать выполнению национальных программ, или нанести ущерб интересам отдельных личностей, но которая тем не менее не затрагивает интересы национальной обороны или внешней политики. В коммерческом секторе понятие критичной информации вводится аналогично — информация, потеря, неправильное использование, модификация или раскрытие которой могут нанести ущерб интересам компании или другой организации, выраженный в материальной (денежный ущерб) или нематериальной (моральный ущерб) форме.

Л

Легендирование — способ защиты информации от технических разведок, предусматривающий преднамеренное распространение и поддержание ложной информации о функциональном предназначении объекта защиты.

Лексикографический индекс [Lexicographical index] — на множестве векторов лексикографический индекс каждого вектора определяется как количество векторов, меньших данного в лексикографическом смысле.

Лечение (выкусывание) [Cure] — процесс удаления вируса из заражен ного им объекта и восстановления состояния этого объекта (файла, загрузочной части диска и т.д.), существовавшего до заражения вирусом.

Лицензиат в области защиты информации — сторона в лицензионном соглашении, передающая право на проведение работ в области защиты информации.

Лицензионное соглашение (договор) в области защиты информации — соглашение (договор) между лицензиаром и лицензиатом, определяющее (определяющий) условия проведения работ в области защиты информации.

Лицензирование в области защиты информации — деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации, оформленная лицензионным соглашением (договором).

Лицензия [License] — разрешение на право продажи или предоставления услуг.

Лицензия в области защиты информации — разрешение на право проведения тех или иных работ в области защиты информации, оформленное лицензионным соглашением (договором).

Личная безопасность [Personnel security] — процедуры, удостоверяющие, что все, кто имеет доступ к критичной информации, получили необходимое разрешение и соответствующие полномочия.

Личная информация [Private information] — информация о гражданах страны или организациях, затрагивающая их интересы, распространение которой возможно лишь в случае согласия на это соответствующих лиц и организаций.

Личная тайна [Privacy] — сведения конфиденциального характера, разглашение которых может нанести материальнфый ущерб отдельному (физическому) лицу. Охрана личной тайны осуществляется ее владельцем.

еще — право индивидуума контролировать и влиять на то, какая информация, относящаяся к индивидууму, может собираться и накапливаться и кем и кому эта информация может быть предоставлена.

Логическая «бомба» [Logic bomb] — программа, которая запускается при определенных временных или информационных условиях для осуществления несанкционированного доступа к информации.

Логическое блокирование [Logical blocking] — бокирование, выполняемое в базах данных на логическом уровне.

Ложная информация [False information] — информация, ошибочно отражающая характеристики и признаки, а также информация о не существующем реально объекте.

Ложное сооружение — объемно-пространственное или плоскостное защитное сооружение, предназначенное для имитации одиночных объектов защиты или элементов объекта прикрытия.

Ложный объект — комплекс ложных сооружений, предназначенный для имитации группового объекта защиты или объекта прикрытия в соответствии с замыслом защиты.

Локальная блокировка [Local lock] — блокировка с целью защиты ресурсов, приписанных области, адресуемой отдельным пользователем. См. *Глобальная блокировка*.

M

Макет — техническое средство, предназначенное для имитации защищаемого изделия (сооружения) при проведении дезинформации.

Мандат [Capability] — разновидность указателя, определяющего путь доступа к объекту и разрешенные над ним операции.

Мандатное управление доступом — концепция (модель) доступа субъектов к информационным ресурсам по грифу секретности разрешенной к пользованию информации, определяемому меткой секретности (конфиденциальности).

Маска — местный предмет или защитное сооружение, предназначенное для скрытия (маскировки) объекта защиты от визуально-оптических и фотографических средств технической разведки, а также от всех видов локации (пеленгации). Маски подразделяются на естественные (лес, кустарник, строения, неровности рельефа и т.д.) и искусственные (инженерные сооружения, системы).

Маскарад [Masquerading] — попытка получить доступ к системе, объекту или выполнение других действий субъектом, не обладающим полномочиями на соответствующее действие и выдающим себя за другого, которому эти действия разрешены.

Матрица доступа [Access matrix] — таблица, отображающая правила доступа субъектов к информационным ресурсам, данные о которых храняться в диспетчере доступа.

еще — таблица, отображающая правила разграничения доступа.

Матрица полномочий [Privilege matrix] — таблица, элементы которой определяют права (полномочия, привилегии) определенного объекта от носительно защищаемых данных.

Машинный код [Computer (machine) code] — двоичный код, используемый для кодирования машинных команд по правилам, предусмотренным в данном типе ЭВМ.

Метаданные [metadata] — данные, описывающие объекты данных (ДСТУ 2874).

Метка грифа [Security label] — указатель, непосредственно связанный с той информацией, к которой он относится, например, как частьпротокола передачи информации.

Метка конфиденциальности [Sensitivity label] — элемент информации, который характеризует степень конфиденциальности информации, содержащейся в объекте доступа.

Метка секретности (конфиденциальности) — элемент информации (бит), который характеризует степень секретности (конфиденциальности) информации, содержащейся в объекте.

Механизм защиты — средства защиты, реализованные для обеспечения служб защиты, необходимых для защиты ЛВС. Например, система аутентификации,

основанная на использовании смарт-карт (которая предполагает, что пользователь владеет требуемой смарт-картой), может быть механизмом, реализованным для обеспечения службы идентификации и аутентификации. Другие механизмы, которые помогают поддерживать конфиденциальность аутентификационной информации, могут также считаться частью службы идентификации и аутентификации.

Механизм контроля доступа [access control mechanism] — оборудование или программное обеспечение, процедуры системы, процедуры администратора и их различные комбинации, которые обнаруживают, предотвращают несанкционированный доступ и разрешают законный в автоматизированных системах.

Механическая генерация — колебания связанной механической системы или вибрация твердых упругих тел.

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

Многоуровневая безопасность [Multilevel security] — класс систем, содержащих информацию с различными уровнями критичности, которые разрешают одновременный доступ к объектам субъектам с различными уровнями прозрачности, но запрещают при этом несанкционированный доступ.

Многоуровневая защита [Multilevel security] — концепция (модель) доступа субъектов с различными правами к объектам различных уровней секретности.

еще — защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

Множественный доступ [Multiple access] — в сетях передачи данных доступ множества станций к широковещательному каналу, позволяющий устранять состязания путем обнаружения конфликта и выполнения повторной передачи.

Модель Белла-Лападула [Bella-LaPadula model] — формальная автоматная модель политики безопасности, описывающая множество правил управления доступом. В этой модели компоненты системы делятся на объекты и субъекты. Вводится понятие безопасного состояния и доказывается, что если каждый переход сохраняет безопасное состояние (то есть переводит систему из безопасного состояния в безопасное), то согласно принципу индукции система является безопасной. Состояние системы считается безопасным, если в соответствии с политикой безопасности субъектам разрешены только определенные типы доступа к объектам (в том числе отсутствие доступа). Для определения, разрешен субъекту доступ к объекту или нет, его уровень прозрачности сравнивается с меткой объекта (уровнем безопасности объекта) и для запрашиваемого типа доступа принимается решение — разрешить доступ или нет. Принятие решения осуществляется на основе двух правил: простого условия безопасности (simple security condition) и *свойства (*-property или star property). Простое условие безопасности разрешает доступ, если уровень прозрачности субъекта не ниже метки критичности объекта. *- условие разрешает доступ, если: для чтения или выполнения — текущий уровень субъекта не ниже метки критичности объекта; для записи или модификации — текущий уровень субъекта не выше метки критичности объекта.

Модель данных [data model] — логическое представление организации данных в базе данных (ДСТУ 2874).

Модель защиты [Protection model] — абстрактное описание комплекса программнотехнических средств и организационных мер защиты от несанкционированного доступа.

Модель защиты информации от несанкционированного доступа — абстрактное (формализованное или неформализованное) описание комплекса организационных мер и программно — аппаратных средств защиты от несанкционированного доступа штатными техническими средствами, являющееся основой для разработки системы защиты информации. Основными способами защиты информации от НСД являются разграничение доступа идентификация и аутентификация пользователя. В свою очередь, основой разграничения доступа (ядро защиты).

Модель нарушителя правил доступа — абстрактное (формализованное или неформализованное) описанием нарушителя правил доступа к информационному ресурсу. Примерами моделей нарушителя правил доступа являются такие программы как троянский конь, логическая бомба, компьютерный вирус и другие.

Модель нарушителя правил разграничения доступа [Security policy violaters model] — абстрактное описание нарушителя правил разграничения доступа.

Модель политики безопасности [security policy model] — формальное представление политики безопасности, разработанной для системы. Оно должно содержать формальное описание определяющих управление, распределение и защиту критической информации.

Модель технических разведок [technical intelligences model] — сведения о методах, средствах и возможностях технических разведок.

еще — описание средств технической разведки,содержащее их технические характеристики и организацию использования в объеме,достаточном для оценки возможностей технической разведки.

Модель угроз информации (техническими средствами) [information treats model (by technical facilities)] — формализованное описание технических каналов утечки, сведения о методах и средствах осуществления угроз информации

Модификация информации — изменение содержания или объема информации на ее носителях при обработке техническими средствами.

Морально-этические нормы в области защиты информации — написанные правила поведения субъектов информационных отношений по сохранению секретной или конфиденциальной информации и ее носителей, основанные на чувстве патриотизме, ответственности и поддержании своего престижа.

Мотор-генератор — развязывающее устройство в цепи электроснабжения, представляющее собой электротехнический комплекс, состоящий из электромотора и электрогенератора, посаженных на одну ось.

Н

Наблюдаемость [Accountability] — возможность для ответственных за защиту информации лиц восстанавливать ход нарушения или попытки нарушения безопасности информационной системы.

Надежность [Reliability] — характеристика способности функционального узла, устройства, системы выполнять при определенных условиях требуемые функции в течение определенного периода времени. Показателя ми надежности являются вероятность безотказной работы, среднее время наработки на отказ, среднее время восстановления.

Надежность программного обеспечения (изделия) [Software (program) reliability] — характеристика способности программного обеспечения выполнять возложенные на него функции при поступлении требований на их выполнение; показатель качества, характеризующий свойства программного изделия выдавать одни и те же результаты при различных условиях функционирования. Надежность и правильность программы не одно и то же.

Нарушение защиты памяти [Memory protection violation] — ошибка, вызывающая программное прерывание и состоящая в том, что ключ защиты области памяти, к которой обращается программа, не совпадает с ключом защиты программы, т.е. ключом защиты области памяти, в которой размещена программа.

Нарушение кода передачи [Transmission code violation] — использование цифр, не принадлежащих коду передачи данных по линиям связи.

Нарушение полномочий [Privilege violation] — попытка пользователя или программы выполнить неразрешенную операцию.

Нарушение целостности [Integrity violation] — искажение содержимого записей файла или базы данных. Происходит вследствие машинных сбоев, программных ошибок, а также ошибочных действий пользователей.

Нарушение целостности информации [information integrity violation] — утрата информации, при ее обработке техническими средствами, свойства целостности в результате ее несанкционированной модификации или несанкционированного уничтожения. Несанкционированная модификация информации может быть случайной (искажение) или умышленной (подделка). Таким образом, по отношению к целостности информации можно дифференцировать дополнительно следующие виды угроз: модификацию, искажение, подделку и уничтожение.

еще — искажение информации, включая ее разрушение или уничтожение

Нарушитель [Attacker] — субъект, действия которого нарушают безопасность информации в рассматриваемой компьютерной системе.

Нарушитель правил доступа — лицо, осуществляющее несанкционированный доступ к информационному ресурсу с использованием штатных технических средств.

Нарушитель правил разграничения доступа [Security policy violation] — субъект доступа, осуществляющий несанкционированный доступ к информации.

Национальный Центр Компьютерной Безопасности (NCSC) США [National Computer Security Center] — организация, поддерживающая и стимулирующая распространение защищенных систем в учреждениях Федерального правительства. Является координирующим органом в области анализа и разработки систем с гарантированной защитой. Первичное название — Центр Компьютерной Безопасности министерства обороны США (DoD Computer Security Center).

Невосстанавливаемая ошибка [Unrecoverable error] — ошибка, последствия которой не могут быть устранены средствами вычислительной системы автоматически и требуют вмешательства оператора.

Независимость данных [data independence] — свойство системы управления базой данных, позволяющее программам быть независимыми от изменений в структуре данных (ДСТУ 2874).

Незаконная деятельность в сфере программного обеспечения [Software piracy] — непредусмотренная документами деятельность лиц, заключающаяся в копировании и распространении программного обеспечения ез соответствующей лицензии.

Незарегистрированный пользователь [Unauthorized user] — пользователь, не состоящий на учете в данной системе коллективного пользования.

Незашифрованный текст [Cleartext] — сообщения или данные, которые доступны непосредственному восприятию.

Некорректируемая ошибка [Uncorrectable error] — ошибка в сообщении, которая не может быть исправлена средствами корректирующего кода.

Некритичная (несекретная) информация [Unclassified information] — классификация данных, не требующих наличия средств защиты от раскрытия.

Ненужная информация [Garbage] — данные в памяти ЭВМ, не подлежащие дальнейшему использованию (устаревшие, недостоверные, дублирующие и т. п.).

Неотображаемый файл [Invisible file] — дисковый файл, который не указывается в справочнике диска на экране дисплея.

Неповторяющаяся (нерегулярная, перемежающаяся, случайная) ошибка [Temporary (intermittent, soft, transiet) error] — несистематическая ошибка, возникающая вследствие самоустраняющихся машинных отказов сбоев и других случайных обстоятельств.

Непосредственная защита [Physical security] — меры, предусматривающие физическую защиту ресурсов от преднамеренных или случайных угроз.

Непреднамеренный (технический)каналутечки информации [unpremeditated (technical) channel ofinformation loss] — технический канал утечки информации, формируемый путем самопроизвольного создания носителей информации и (или) сред их распространения.

Непрерывность защиты — принцип защиты, заключающийся в организации защиты объекта на всех стадиях его жизненного цикла: в период разработки, изготовления (строительства), испытаний, эксплуатации и утилизации.

Несанкционированный (неавторированный) доступ (НСД) [Unauthorized (illegal) access] — преднамеренное обращение пользователя к данным, доступ к которым ему не разрешен, с целью их чтения, обновления или разрушения.

Несанкционированный доступ к информации [Unauthorized access to information] — доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

еще — доступ к информации, осуществляемый штатными техническими средствами с нарушением установленных правил. Несанкционированный доступ может создать любой из видов угроз безопасности информации: утечку (рассекречивание), нарушение целостности или блокирование.

Несекретная информация — информация, которая не представляет собой государственную, служебную, коммерческую или личную тайны и может быть опубликована в открытой печати. Несекретная информация не защищается от утечки, так как не содержит в себе каких-либо тайн, но в случае если она представлена в форме документов (библиотеки) или банка данных ЭВМ она может и должна защищаться от нарушения целостности и блокирования.

Нечувствительность к изменению данных — см. *Толерантность.*

Нечувствительность к отказам [Fault tolerance] — свойство программы или системы сохранять правильность функционирования при наличии ошибок или отказов.

Нештатная ситуация — ситуация, возникающая в процессе работы вычислительной системы, но не предусмотренная программной документацией.

Новости [news] — протокол передачи сетевых новостей (NNTP) для распространения новостей в Usenet . Usenet — это система асинхронного обсуждения текстов по различным тематикам, называемым группами новостей (*newsgroups)*.

Норма акустической защиты (защищенности) выделенного помещения — количественное значение параметра акустической защиты (защищенности) которое необходимо достичь (которое достигнуто) в результате проведения акустической защиты в зависимости от группы выделенного помещения.

Норма безопасности — количественное значение критерия безопасности информации, устанавливаемое в зависимости от категории безопасности.

Носитель аппаратуры технической разведки — механическое транспортное средство или живой организм (в том числе человек), предназначенные для установки и перевозки (переноски) аппаратуры технической разведки в различных средах. По типу носителей аппаратуры технической разведки различают наземную, воздушную, космическую и морскую (наводную и подводную) разведки.

Нумерационное кодирование [Enumerative coding] — представление последовательности сообщений источника последовательностью целых чисел.

О

Область [Domain] — уникальный контекст (например, параметры контроля доступа) исполнения программы, множество объектов, к которым субъект может иметь доступ. Имеет иерархическую структуру.

Область блокирования [Locking unit] — часть базы данных (запись, область, файл), открытая для монопольной обработки одной программой и недоступная до момента закрытия другим программам.

Обман [Spoofing] — намеренная попытка вынудить пользователя или ресурс системы выполнить неправильное действие.

Обмен данными [Data commuunication] — процедура приема и передачи данных, включая кодирование, декодирование буферизацию и проверку.

Обнаружение и исправление ошибок [Error detection and correction] — для обнаружения ошибок либо в данные вводится определенная избыточность, позволяющая их контролировать, либо процесс вычислений дублируется. Некоторые ошибки, связанные с передачей данных, могут быть исправлены путем повторной пересылки этих данных. В других случаях приходится применять системы с прямым исправлением ошибок.

Обнаружение объекта — процесс функционирования средства технической разведки, в результате которого фиксируются технические демаскирующие признаки объекта и делается заключение о его наличии.

Обработка данных [data processing] — систематическое выполнение операций над данными (ДСТУ 2874).

Обратный ассемблер [Disassembler] — программа, служащая вспомогательным средством отладки и переводящая программу в машинных кодах обратно на язык ассемблера.

Обход системы — попытка пользователя получить доступ к данным в обход предусмотренных в системе средств защиты от несанкционированного доступа.

Общедоступная информация [Public data] — информация, сокрытие которой недопустимо и которую может получить любой гражданин страны.

Объект [Object] — организационное и территориальное объединение сил и средств, предназначенных для совместного осуществления управленческой, научно-технической, производственной или коммерческой деятельности. К объектам относятся государственные и частные учреждения и предприятия, научно-исследовательские институты, конструкторские бюро, опытные и серийные заводы, испытательные центры, полигоны и т.п.

еще — пассивный компонент системы, хранящий, принимающий или передающий информацию. Доступ к объекту подразумевает доступ к содержащейся в нем информации. Примеры объектов: записи, блоки, страницы, сегменты, файлы, директории и программы, а также отдельные биты, байты, слова, поля; различные устройства (терминалы, принтеры, дисководы и т.д.); различные сетевые устройства (отдельные узлы, кабели и т.д.).

Объект безопасности [Security object] — пассивная системная составляющая, к которой применяется методика безопасности.

Объект вычислительной техники ОВТ — стационарный или подвижный объект, который представляет собой комплекс средств вычислительной техники, предназначенный для выполнения определенных функций обработки информации. К объектам вычислительной техники относятся автоматизированные системы (АС), автоматизированные рабочие места (АРМ), информационно — вычислительные центры (ИВЦ) и другие комплексы средств вычис-

лительной техники (см. ГОСТ 34.003-90). К объектам вычислительной техники могут быть отнесены также отдельные средства вычислительной техники, выполняющие самостоятельные функции обработки информации.

Объект доступа [Access object] — единица информационного ресурса, к которой осуществляется доступ штатными техническими средствами.

еще — единица ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Объект защиты — обобщающий термин для всех форм существования информации, требующих защиты от технических разведок. По своему составу объекты защиты могут быть единичными и групповыми.

Объект информатики — стационарный или подвижный объект, который представляет собой комплекс технических средств обработки информации, предназначенный для выполнения определенных функций. К объектам информатики могут быть отнесены также отдельные технические средства обработки информации, выполняющие определенные функции обработки информации.

Объект технической разведки — объект, используемый технической разведкой как источник разведывательной информации.

Объектная программа [object program] — выходная программа, пригодная для машинного выполнения (ДСТУ 2873).

Однозначно декодируемый код [Uniquely decodable code] — код, слова которого образуют однозначно дешифрируемое множество. См. однозначно дешифрируемое множество.

Одноступенчатая система защиты [Key to the door] — система защиты, в которой единственный ключ обеспечивает доступ к программному обеспечению.

Оконечное шифрование [Endtoend encipherментt] — шифрование данных в реальной оконечной системе источнике данных, в соответствующее дешифрование, которое производится в реальной оконечной системе приемнике данных.

«Оранжевая книга» [Orange book] — полное название "Department of Defence Trusted Computer System Evalution Criteria" DOD 5200.28STD ("Критерий оценивания безопасности компьютерных систем министерства обороны"). Это американский (США) стандарт оценивания безопасности компьютерных систем, устанавливающий четыре класса A, B, C и D уровней доверительности (или уверенности в безопасности) для конкретных приложений, разрабатываемых и используемых в интересах правительства.

Опасная зона I — пространство вокруг технического средства обработки информации, в пределах которого на случайных антеннах наводится опасный сигнал выше допустимого нормированного уровня. В зоне I запрещается размещение случайных антенн, имеющих выход по токопроводящим коммуникациям за пределы контролируемой зоны.

Опасная зона 2 — пространство вокруг технического средства обработки информации, в пределах которого отношение опасный сигнал/помеха для составляющих напряженности электромагнитного поля превышает допустимое нормированное значение.

Опасный сигнал — параметр технического демаскирующего признака объекта, являющийся носителем секретной или конфиденциальной информаии.

Операционная безопасность [Operational data security] — защищенность данных от модификации, разрушения или разглашения (случайных, неавторизованных, либо преднамеренных) во время выполнения операций ввода, обработки или вывода.

Операционная система (ОС) [Operating system (O.S.)] — основная часть программного обеспечения, которая координирует и управляет ресурсами ЭВМ и данными.

Оптико-электронный (лазерный) канал утечки акустической (речевой) информации — канал утечки акустической (речевой) информации, обусловленный процессом зондирования лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекла окон, картин, зеркал и т.д.), модуляции этого луча по закону вибрации поверхностей и приемом отраженного (зеркально или диффузно) луча оптическим (лазерным) приемником.

Орган по сертификации в области защиты информации — орган, проводящий сертификацию защищенных изделий, технических средств и способов защиты информации на соответствие конкретному стандарту или другому документу. Орган по сертификации может сам производить испытания и контроль за испытаниями или же осуществлять надзор за этой деятельностью, проводимой по его поручению другими органами.

Организационная защита информации — защита информации при ее обработке техническими средства-

ми, осуществляемая путем принятия административных мер. Административные меры включают выбор места расположения объекта, не подверженного внешним воздействиям, организацию контролируемой (проверяемой) зоны, выполнение правил учета, хранения и обращения секретных (конфиденциальных) документов на различных носителях и другие меры.

Организационное мероприятие по защите информации — мероприятие по защите информации, предусматривающее использование маскирующих свойств окружающей среды и установление временных, территориальных и пространственных ограничений на условия использования и режимы работ объекта.

Организационно-техническая форма защиты информации — защита информации, предусматривающая применение руководящих, нормативных и методических документов, лицензирование деятельности в области защиты информации, сертификацию защищенных изделий, технических средств и способов защиты, создание на объектах систем защиты информации и аттестацию этих объектов.

Организационный контроль эффективности защиты информации — контроль эффективности защиты информации путем проверки соответствия состояния, организации, наличия документов, полноиты и обоснованности мероприятий по защите информации требованиям организационно — распорядительных и нормативных доркументов.

Основные технические средства[general technical facilities] — средства и системы формирования, передачи, приема, преобразования, отображения и хранения информации с ограниченным доступом.

Отказ [Failure] — ситуация, в которой какаято часть вычислительной системы оказывается неспособной выполнять возлагаемые на нее функции.

Отказ в обслуживании [Denial of service] — любое действие или последовательность действий, которая приводит любую часть системы к выходу из строя, при котором та перестают выполнять свои функции. Причиной может быть несанкционированный доступ, задержка в обслуживании и т.д.

еще — прекращение санкционированного доступа к ресурсам или задержка операций, критичных по времени выполнения.

Отказоустойчивая система [Faulttolerant system] — вычислительная система, которая при возникновении отказа сохраняет свои функциональные возможности в полном или уменьшенном объеме. Отказоустойчивость обычно обеспечивается сочетанием избыточности системы и наличия процедур обнаружения и устранения ошибок.

Открытый текст — имеющая смысл (допускающая возможность восстановления семантического содержания) информация, участвующая в процессе шифрования.

Охраняемые сведения — сведения, составляющие государственную, служебную, коммерческую или личную тайны, на распространение которых накладываются ограничения соответствующими заинтересованными органами.

Оценка защиты [Security evaluation] — проверка системы с целью определения степени ее соответствия установленной модели защиты, стандарту обеспечения защиты и техническим условиям.

Оценка качества программного изделия [Program quality estimation] — комплекс мероприятий, включающий выбор показателей качества, отбор или разработку методов определения количественных значений этих показателей, установление базовых значений показателей, расчет реальных значений показателей, сравнение базовых значений с расчетными.

Оценка риска [Risk assessment] — количественная или качественная оценка повреждения, которое может произойти, если вычислительная система не защищена от определенных угроз. Количественная оценка риска может рассчитываться на основе финансовых потерь, которые могут иметь место, если каждая конкретная угроза будет приводить в действие любой из возможных механизмов уязвимости системы.

Ошибка в данных [Data error] — ошибочное представление одного или нескольких исходных данных Может стать причиной аварийного завершения программы либо оказаться необнаруженной, но результаты нормально завершившейся программы будут при этом неверными.

Ошибка четности [Parity error] — ошибка в данных, обнаруживаемая в процессе их хранения или передачи путем контроля на четность.

П

Пакеты-убийцы — метод вывода из строя системы путем посылки ей Ethernet- или IP-пакетов, которые используют ошибки в сетевых программах для аварийного завершения работы системы.

Память с защитой [Protected storage] — память, имеющая специальные средства защиты от несанкционированного доступа к любой из ее ячеек.

Параметр акустической защиты (защищенности) выделенного помещения — показатель, который принимается для оценки акустической защиты (защищенности) выделенного помещения. В качестве параметра акустической защиты (защищенности) выделенного помещения принято отношение уровня речевого сигнала, проникающего за пределы выделенного помещения, к уровню стабильного шумового фона в той же точке (отношение сигнал/шум): $R_з = L_c - L_ш$, где $R_з$ — параметр акустической защиты (защищенности), дБ; L_c — уровень сигнала, дБ; $L_ш$ — уровень шума, дБ.

Параметр технического демаскирующего признака — показатель технического демаскирующего признака объекта, используемый технической разведкой для получения разведывательной информации. К параметрам прямых демаскирующих признаков относятся напряженность магнитного и электромагнитного полей по сравнению с магнитным (электро-магнитным) фоном окружающей среды, уровень электромагнитных наводок на вспомогательных технических средствах и системах, интенсивность (звуковое давление) акустического поля и т.д.,а параметрами косвенных демаскирующих признаков могут быть геометрические размеры тех или иных объектов, контрастность их освещенности, уровень радиоактивного или химического заражения окружающей местности по сравнению с естественным фоном и другие параметры.

Параметрический канал утечки акустической (речевой) информации — канал утечки акустической (речевой) информации, обусловленный параметрическим преобразованием акустического (речевого) сигнала в нелинейном акустическом поле, создаваемом направленным излучением мощных высокочастотных бигармонических колебаний (волн накачки). Нелинейное взаимодействие акустических сигналов и разностной частоты волн накачки (так называемой вторичной волны) способствует созданию острой (без боковых лепестков) диаграммы направленности излучения, обеспечивающей передачу акустической информации на большие расстояния.

Пароль [Password] — средство идентификации доступа, представляющее собой кодовое слово в буквенной, цифровой или буквенно-цифровой форме, которое вводится в ЭВМ перед началом диалога с нею с клавиатуры терминала или при помощи идентификационной (кодовой) карты.

еще — секретный признак, подтверждающий право доступа; обычно это строка символов. Идентификатор пользователя, который является его секретом. Служит для защиты данных и программ от несанкционированного доступа.

Пассивная угроза [Passive threat] — возможность несанкционированного доступа к информации без изменения режима функционирования системы.

Пассивное скрытие [passive hiding] — способ технической защиты информации, состоящий в ослаблении энергетических характеристик сигналов, полей или в уменьшении концентраций веществ.

Пассивное техническое средство защиты — техническое средство защиты, обеспечивающее скрытие объекта защиты от технических разведок путем поглащения, отражения или рассеивания его излучений. К пассивным техническим средствам защиты относятся маски различного назначения, экранирующие устройства и сооружения, разделительные устройства в сетях электроснабжения, защитные фильтры и т.д.

Патент [Patent] — гарантия со стороны правительства, данная изобретателю или его доверенному лицу и дающая привилегию в виде исключительного права на реализацию, использование или продажу изобретения в течение определенного срока (обычно 20 лет).

Переполнение-SYN — метод вывода системы из строя путем посылки ей такого числа SYN-пакетов, которое не может обработать сетевой драйвер. Смотрите пакеты-убийцы.

Перестановка [Permutation] — криптографическая операция, связанная с изменением порядка следования отдельных битов или символов в блоке данных. См. подстановка.

Пересылка файлов [File transfer] — процедура перемещения содержимого всего файла или его части между открытыми системами.

Перехват сообщений [Message wiretapping] — несанкционированное подключение специального терминала к линии связи, прием и использование сообщений, циркулирующих между абонентскими пунктами и ЭВМ.

Период доступа [Access period] — временной интервал, в течение которого действуют права доступа. В основном этот период определяется в днях или неделях.

Персональный идентификационный номер [Personal Identification Number (PIN)] — персональный код некоторого лица, обеспечивающий ему возможность входа в систему с управляемым доступом.

Плагин [Plug-in] — набор динамически подключаемых библиотек, используемых для увеличения функциональных возможностей основной программы, такой как WWW-браузер. Они обычно используются для того, чтобы позволить WWW-браузеру отображать и обрабатывать данные в различных форматах, или чтобы добавить новые возможности отображения стандартных форматов.

План обеспечения непрерывной работы и восстановления функционирования, [Contingency plan (backup plan, recovery plan)] — план реагирования на опасные ситуации, резервного копирования и последующих восстановительных процедур, являющийся частью программы защиты и обеспечивающий доступность основных ресурсов системы и непрерывность обработки в кризисных ситуациях.

Побитовый подсчет [Bit counting] — метод защиты от копирования, при котором диск распознается как оригинал, если некоторый трек (или другая область) содержит определенное число битов.

Побочное электромагнитное излучение (ПЭМИ) — нежелательное информационное электромагнитное излучение, возникающее в результате нелинейных процессов в электрических цепях при обработке информации техническими средствами и приводящие к утечке информации.

Повреждение данных [Data corruption] — нарушение целостности данных.

Повторное использование объекта [Object reuse] — переназначение и повторное использование пространства памяти (например, страницы, фрейма, сектора диска, магнитной ленты), которое ранее содержало в себе один или несколько объектов. Для поддержания безопасности это пространство при выделении его под новый объект не должно содержать информации старых объектов.

еще — предоставление некоторому субъекту доступа к магнитной среде, содержащей один и более объектов. Будучи доступной для субъекта, магнитная среда может в то же время содержать остатки данных от объекта, содержавшегося на этом месте ранее.

Подглядывание из-за плеча — кража паролей или PIN-кодов путем наблюдения за их набором на клавиатуре.

Подделка информации [Forgery] — умышленная несанкционированная модификация информации при ее обработке техническими средствами с целью получения определенных выгод (преимуществ) перед конкурентом или нанесения ему ущерба.

еще — предумышленное искажение информации.

Подмена [Mascquerade] — поведение пользователя, пытающегося выдать себя за другого пользователя.

Подстановка [Substitution] — криптографическая операция, связанная с замещением блока другим и использующая определенный код. См. перестановка.

Подстановка трафика [Traffic padding] — установление поддельных соединений, генерация фальшивых блоков данных и (или) отдельных фальшивых данных внутри блоков данных.

Подтверждение подлинности [Authentication exchange] — механизм, направленный на подтверждение подлинности и предусматривающий обмен информацией.

Пожаростойкость технического средства обработки информации — устойчивость технического средства обработки информации против возгорания (самовозгорания) при экстремальных климатических и погодных условиях.

Показатель защищенности средстввычислительнойтехники [Protection criterion of computer system] — характеристика средств вычислительной техники, отражающая защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники.

Показатель эффективности защиты информации — параметр технического демаскирующего признака объекта защиты применительно к которому устанавливаются требования и/или нормы по эффективности защиты информации.

Поле защищенности средств вычислительной техники [Protection criterion of computer system] — характеристика средств вычислительной техники, устанавливающая принадлежность вычислительной техники определенному классу защищенности средств вычислительной техники.

Полиномиальный код [Polynomial code] — код с обнаружением ошибок, в котором контрольные разряды являются остатком от деления передаваемых разрядов на фиксируемое число.

Политика безопасности [security policy] — набор законов, правил и практического опыта, на основе ко-

торых строится управление, защита и распределение критичной информации.

Политика информационной безопасности — совокупность документов, определяющих управленческие и проектные решения в области ЗИ.

Полномочия — право пользователя (терминала, программы, системы) осуществлять те или иные процедуры над защищенными данными.

Полномочное управление доступом [Mandatory access control] — способ управления доступом к объектам, основанный на степени секретности или критичности информации (представленной специальными метками), содержащейся в объекте и формальной проверке полномочий и прав субъекта при доступе к информации данного уровня критичности еще — разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

Получатель информации — материальный объект или субъект, воспринимающий информацию во всех формах ее проявления с целью дальнейшей ее обработки и использования. Источниками и получателями информации могут как люди, так и технические средства, которые накапливают, хранят, преобразуют, передают или принимают информацию.

Получение разведывательной информации — процесс, складывающийся из добывания разведывательных данных и получения сначала разведывательных сведений, а затем итоговой разведывательной информации в форме, удобной для восприятия человеческим сознанием. Восприятие человеком любой информации, в том числе разведывательной информации потребителем, осуществляется поэтапно и состоит из чувственного познания (восприятие с помощью органов чувств) и абстрактного мышления, заключающегося в опосредованном, отвлеченном и обобщенном отражении объектов и явлений внешнего мира. Высшими формами абстрактного мышления является язык (речь) и письменность, представляющие собой средства материального выражения мысли. Обработка разведывательных данных и сведений и получение разведывательной информации может осуществляться как вручную, так и с использованием технических средств.

Пользователь (потребитель) информации — субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею

еще — любое лицо или любой объект, которые могут пересылать команды или сообщения в систему обработки данных либо получать их из нее (ДСТУ 2874)

еще — субъект информационных отношений, обладающий правом пользования доверенным ему информационным ресурсом.

Помеха технической разведке — физический процесс или действие, обеспечивающее полное подавление или существенное снижение возможностей технической разведки.

Помехи [Noise, interference] — возмущения в канале связи, искажаю щие передаваемое сообщение.

Помехозащищенность [Noise protection] — способность ЭВМ сохранять качество функционирования при воздействии внешних помех и наличии дополнительных средств защиты от помех, не относящихся к принципу действия или построения машины.

Помехоустойчивое кодирование [Noiseless coding] — в теории связи использование кода, повышающего эффективность системы связи, в которой помехи отсутствуют вообще или незначительны. Помехоустойчивое кодирование в общем виде идентично кодированию источника.

Помехоустойчивость [Noise immunity] — способность ЭВМ сохранять качество функционирования при воздействии внешних помех в отсутствие дополнительных средств защиты от помех, не относящихся к принципу действия или построения машины.

Попытка доступа к информации неавторизованная [Hacking] — попытка получить доступ к информации за счет обхода (обмана) средств контроля доступа в сети.

Порча данных [Data contamination] — изменение данных злоумышленное или случайное в вычислительной системе.

Посредник [PROXY] — приложение, выполняемое на шлюзе, которое передает пакеты между авторизованным клиентом и внешним хостом. Посредник принимает запросы от клиента на определенные сервисы Internet, а затем, действуя от имени этого клиента (т.е. выступая его посредником), устанавливает соединение для получения запрошенного сервиса. Все шлюзы прикладного уровня используют связанные с приложениями программы-посредники. Большинство шлюзов сеансового уровня ис-

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

Почта электронная [Electronic mail (computer mail)] — система пересылки сообщений между пользователями вычислительных систем, в которой ЭВМ берет на себя все функции по хранению и пересылке сообщений. Для осуществления такой пересылки отправитель и получатель (получатели) не обязательно должны одновременно находиться у терминалов и необязательно должны быть подключены к одной ЭВМ.

Почтовые «бомбы» — блокирование сайта путем вывода из строя почтового сервера посылкой огромного числа писем. Используется для предотвращения получения сайтом писем в ходе атаки или для мести.

Правила доступа — правила, установленные для осуществления доступа субъекта к информационному ресурсу с использованием штатных технических средств.

Правила разграничения доступа [Security police] — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Право [Author right, copyright] — исключительное право, предоставляемое законом автору или его представителю, на воспроизведение, публикацию и копирование оригинальной работы.

Правовая форма защиты информации — защита информации, базирующаяся на применении статей конституции и законов государства, положений гражданского и уголовного кодексов и других нормативно-правовых документов в области информатики, информационных отношений и защиты информации. Правовая форма защиты информации регламентирует права и обязанности субъектов информационных отношений, правовой статус органов, технических средств и способов защиты информации и является базой для создания морально-этических норм в области защиты информации.

Преднамеренный (технический)канал утечки информации [premeditated (technical) channel ofinformation loss] — технический канал утечки информации, формируемый путем целенаправленного создания носителей информации и (или) сред их распространения.

Предоставление авторских полномочий [Authorization] — предоставление администратором системы конкретным лицам прав владения, позволяющих последним использовать транзакции, процедуры или всю систему в целом.

Предоставление права на доступ [Authorization] — выдача разрешения (санкции) на использование определенных программ и данных.

Предписание на изготовление — документ, содержащий требования по обеспечению защищенности технические средства обработки информации в процессе его производства.

Предписание на эксплуатацию — документ, содержащий требования по обеспечению защищенности технического средства обработки информации в процессе его эксплуатации.

Предупредительная защита [Disincentive protection] — организационные меры защиты от копирования, предусматривающие суровый штраф или угрозу штрафа лицу, которое пытается несанкционированно копировать программу или файл.

Приватность данных [Data privacy] — статус данных, состоящий в их доступности только владельцу или ограниченной группе пользователей; гарантированная системой доступность к данным со стороны определенного лица или группы лиц.

Привилегии [Privilege] — права пользователя или программы, состоящие в доступности определенных объектов и действий в вычислительной системе.

Привилегированная команда [Privileged instruction] — команда, которая может быть выдана только тогда, когда вычислительная система находится в одном из высокоприоритетных или в самом приоритетном состоянии.

Привилегированный пользователь [Privileged (authorized) user] — пользователь, имеющий по сравнению с другими пользователями большие права и привилегии при работе с вычислительной системой (например, более высокий приоритет highpriority uuser).

Приоритет прерываний [Interrupt priority] — характеристика важности, присваиваемая программным прерываниям. Как правило, система может одновременно обслуживать только одно прерывание, однако в некоторых случаях скорость поступления прерываний превышает скорость обслуживания. В подобной ситуации при помощи системных средств управления можно установить такие маски прерываний, которые будут подавлять некоторые прерывания при наличии более важных прерываний.

Прицельная помеха — помеха, ширина спектра частот которой соизмерима с шириной полосы частот приемного устройства аппаратуры разведки или технического демаскирующего признака.

Программа TEMPEST — программа изучения и анализа побочных электронных сигналов, излучаемых электрическим и электронным оборудованием.

Программа проверка правильности исходных данных [Datavet program] — программа, с помощью которой выполняется контроль входных данных на соответствие заданным характеристикам и целостность.

Программа самозагрузки [Boot] — минимальное множество команд, необходимое для загрузки операционной системы.

Программная «бомба» — тайное встраивание в программу команд, которые должны срабатывать один или несколько раз при определенных условиях. Существуют варианты с "логической" или "временной" бомбой.

Программная закладка [program bug] — несанкционировано внедренная программа, осуществляющая угрозу информации.

Программная интерпритация — способ защиты управляющей программы от несанкционированной модификации путем загрузки ее в измененной форме с помощью кодового оптимизатора.

Программная среда [programming environment] — интегрированная совокупность технических и программных средств, при помощи которых осуществлятся разработка программ (ДСТУ 2873).

Программное средство защиты информации — специальная программа, входящая в комплект программного обеспечения и предназначенная для защиты информации.

Программные средства [software] — средства, которые состоят из программ и документации, относящейся к их функционированию (ДСТУ 2873).

Проникновение [Penetration] — успешное преодоление механизмов защиты системы.

Просмотр [Browsing] — поиск информации, нередко преследующий цель получения несанкционированного доступа к конфиденциальным данным и представляющий в этом случае угрозу для вычислительной системы.

Противоречивая информация [Contradictory information] — информация, отдельные элементы которой противоречат друг другу, не согласуются друг с другом.

Противоречивость данных [Data inconsistency] — состояние базы данных, при котором дублирующие данные не равны либо значения данных не соответствуют области их определения.

Протокол [Protocol] — согласованная процедура передачи данных между различными объектами вычислительной системы; обычно употребляется в сочетании ISO protocol протокол Международной организации по стандартизации.

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

Протокол Gopher — разработан для того, чтобы позволить пользователю передавать текстовые и двоичные файлы между компьютерами в сети.

Протокол Telnet — используется для терминального (возможно удаленного) подключения к хосту.

Протокол безопасной передачи данных [SSL] — разработан Netscape Communications, Inc. Этот протокол использует межконцевое шифрование трафика на прикладном уровне.

Протокол передачи гипертекста [HTTP] — базовый протокол WWW, использующийся для передачи гипертекстовых документов.

Протокол передачи файлов [FTP] — используется для передачи файлов по сети.

Профиль выполнения [execution profile] — представление абсолютной или относительной частоты выполнения или времени выполнения команд программы (ДСТУ 2873).

Профиль защиты — документ, описывающий задачи обеспечения ЗИ в терминах функциональных требований и требований гарантированности.

Проход через систему защиты (обходной путь) [Trapdoor] — 1) Блок, скрытый в большой программе, который разрешает пользователю преодолеть систему защиты или учета ресурсов системы в штатном режиме; 2) Блок обхода, встроенный в систему шифрования.

Процедурная безопасность [Procedural security] — ограничения со стороны управляющих органов; операционные, административные и учетные процедуры; соответствующие способы управления, используемые с целью обеспечения требуемого уровня безопасности для критичных к защите информации данных.

Процесс [process] — выполняющаяся программа. См. Также domain и subject.

Процессор [processor] — функциональное устройство, обеспечивающее конкретное применение некоторой совокупности команд (ДСТУ 2874).

Псевдослучайный процесс [Pseudorandom process] — процесс, кажущий ся случайным. Таким может быть детерминированный процесс, который в принципе не может быть случайным, но вместе с тем способен демонстрировать ряд проявлений случайностей в любой необходимой степени (в зависимости от принятой структуры), а потому может служить заменителем случайного процесса и называться псевдослучайным.

Психологический барьер [Psychological barrier] — барьер, возникающий между пользователем и новой системой, вызываемый, как правило, боязнью трудностей при переходе на новую систему, неизвестностью того, будет ли она лучше старой системы

Путь доступа [access path] — последовательность элементов данных, которые используются системой управления базой данных для доступа к записям или другим элементам данных, хранящимся в базе данных (ДСТУ 2874).

Путь проникновения [Penetration route] — последовательность не санкционированных действий пользователя при его проникновении в защищенную вычислительную систему.

Р

Работа (процесс) — изыскательские, проектные, научно-исследовательские, опытно-конструкторские и иные работы (в том числе работы студентов дипломников и диссертантов), технологические процессы, а также боевые действия войск и сил флота.

Радиус (опасной) зоны — радиус сферы, охватывающий зону 1 или зону 2.

Разведывательная информация — информация, полученная в результате отбора, сопоставления, логической увязки и обобщения разведывательных данных и сведений в соответствии с заданием потребителя.

Разведывательные данные — зарегистрированные и/или зафиксированные средством технической разведки технические демаскирующие признаки объекта.

Разведывательные сведения — смысловая и фактографическая информация об объекте разведки, получаемая в результате обработки разведывательных данных.

Развязывающие устройства и приспособления — устройства и приспособления в цепях электроснабжения, линиях связи и других токопроводящих коммуникациях, предназначенные для предотвращения выхода опасного сигнала за пределы контролируемой зоны объекта. К развязывающим устройствам и приспособлениям относятся моторгенераторы, фильтры различного назначения и изолирующие вставки.

Разграничение доступа — наделение каждого пользователя (субъекта доступа) индивидуальными правами по доступу к информационному ресурсу и проведению операций по ознакомлению с информацией, ее документированию, модификации и уничтожению. Разграничение доступа может осуществляться по различным моделям, построенным по тематическому признаку или по грифу секретности разрешенной к пользованию информации.

еще — совокупность методов, средств и мероприятий, обеспечивающих защиту данных от несанкционированного доступа пользователей.

Разделение привилегий [Privilege sharing] — принцип открытия механизма защиты данных, при котором для доступа к ним необходимо указать не один, а два пароля (например, двумя лицами).

Разнообразие защиты — принцип защиты, предусматривающий исключение повторяемости в выборе путей реализации замысла защиты, в том числе с применением типовых решений.

Разрушение информации [Data erasing] — стирание информации, хранящейся в памяти ЭВМ.

Разряд защиты [Guard digit] — один из дополнительных разрядов промежуточных результатов, обеспечивающих сохранение точности.

Распознавание объекта — процесс функционирования средства технической разведки, в результате которого измеряются параметры демаскирующего признака объекта и делается заключение о его характеристиках (производится классификация).

Распределенная база данных [distributed database] — база данных, физически распределенная на две или больше компьютерные системы (ДСТУ 2874).

Распределенная случайная антенна — случайная антенна с распределенными параметрами. К распределенным случайным антеннам относятся кабели, провода, металлические трубопроводы и другие токопроводящие коммуникации.

Расшифрование (информации) [Decryption] — процесс преобразования зашифрованных данных в открытые при помощи шифра.

еще — см. *Дешифрование.*

Регистрация открытого ключа [Public key registry] — процесс фиксации открытых ключей, обеспечивающих достоверную информацию лицу, осуществляющему запрос, с целью предотвратить фальсификацию значения открытого ключа.

Режим обеспечения безопасности [Security processing mode] — описание всех категорий допусков всех пользователей в привязке ко всем категориям защиты информации, которая должна храниться и обрабатываться в системе.

Режимное предприятие (учреждение) — групповой объект защиты, представляющий собой предприятие (учреждение), информация о функциональной деятельности которого и получаемых результатах требует защиты от технических разведок.

Резидентный [Resident] — постоянно присутствующий в оперативной памяти.

Реляционная модель данных [relational model] — модель данных для представления данных с реляционной структурой.

Реляционная структура [relational structure] — структура данных, в которой данные представляются как таблицы соотношений (ДСТУ 2874).

Ресурс [Resource] — любой из компонентов вычислительной системы и предоставляемые ею возможности.

Речевая информация — акустическая информация, источником которой является человеческая речь. Речевая информация обладает высокой семантической связью и имеет наивысшую информативность.

Речевой сигнал — сложный акустический сигнал, источником которого является человеческая речь. Спектральная плотность речевого сигнала близка к спектральной плотности розового шума.

Риск [Risk] — возможность проведения захватчиком успешной атаки в отношении конкретной слабой стороны системы.

Робастность [Robustness] — мера способности вычислительной системы восстанавливаться при возникновении ошибочных ситуаций как внешнего, так и внутреннего происхождения.

Розовый (акустический) шум — сложный акустический сигнал, уровень спектральной плотности которого убывает с повышением частоты с постоянной крутизной, равной 3 дб по октаву во всем диапозоне частот.

С

Самоадаптация [Selfadapting] — способность системы автоматически изменять свои функциональные характеристики в ответ на изменения внешней среды.

Самодиагностика [Selfdiagnosis] — способность системы самостоятельно обнаруживать, локализовывать и анализировать ошибки и отказы.

Самокодирование [Intrinsic fingerprint] — кодирование информации с использованием самой информации в качестве ключа.

Самоконтролируемый код [Selfchecking code] — избыточный код, расшифровка которого автоматически приводит к обнаружению или исправлению ошибок.

Самоконтроль [Selfchecking] — способность системы автоматически контролировать процесс своего функционирования и определенным образом реагировать на возникновение отказов.

Санкционирование [Authorization] — предоставление права пользования услугами системы, например, права доступа к данным.

Санкционированное (разрешенное) состояние [Authorized state] — состояние, при котором непривилегированная программа имеет доступ к ресурсам, недоступным в других условиях.

Санкционированный анализ программы [Authorized program analysis] — анализ, выполняемый для установления расхождения между техническими требованиями и реальными возможностями программы.

Санкционированный вызов [Authorized call] — вызов системы, программы или данных, разрешенный данному пользователю. Как правило, реализуется путем ввода и проверки пароля.

Санкционированный доступ (к информации) [Authorized access to information] — доступ к информационному ресурсу, который осуществляется штатными техническими средствами в соответствии с установленными правилами.

еще — доступ к информации, не нарушающий правила разграничения доступа.

Сбой [Failure] — кратковременный, неустойчивый отказ оборудования, возникающий вследствие неста-

бильности питания, ненадежности соединений, попадания частиц в подвижные части, несоблюдения температурных режимов и т. п.

Сбор данных [Data collection] — процесс идентификации и получения данных от различных источников, группирования полученных данных и представление их в форме, необходимой для ввода в ЭВМ.

Сбор знаний [Knowledge acquisition] — получение информации о предметной области от специалистов-экспертов и представление ее в форме, необходимой для записи в базу знаний.

Свертка [Folding] — простой метод хеширования ключа, согласно которому ключ разбивается на несколько частей, сложение которых дает адрес. Коэффициент свертки равен отношению области определения соответствующей функции хеширования к размеру области ее значений.

Сверточный код [Convolutional code] — код, в каждый момент времени порождающий очередную порцию кодовых символов, называемую кодовым подблоком, при поступлении на вход кодера очередной порции информационных символов, называемую информационным подблоком.

Свойство синхронизируемости [Synchronizing property] — свойство кода, состоящее в том, что декодер, начав работу с произвольного символа: кодовой последовательности, может определить начало очередного кодового слова и приступить к восстановлению последовательности сообщений.

Секретная информация [secret information] — информация, которая представляет собой государственную или служебную тайны и охраняется государством. В зависимости от величины политического или экономического ущерба, который может быть нанесен интересам государства в случае разглашения секретной информации она может иметь гриф особой важности, совершенно секретно или секретно.

еще — информация с ограниченным доступом, которая содержит сведения, составляющие предусмотренную законом тайну и доступ к которой определен правовыми нормами.

Секретность (конфиденциальность) информации — свойство информации при ее обработке техническими средствами, обеспечивающее предотвращение несанкционированного ознакомления с ней или несанкционированного документирования (снятия копий).

Секретность данных [Data privacy] — ограничение, накладываемое автором на доступ к его информации другим лицам. Оформляется присваиванием информации определенного грифа и осуществляется закрытием ее паролем, шифрованием и другими методами.

Секретные данные [Confidential data] — закрытые данные, которым присвоен определенный гриф (степень) секретности.

Семантическая ошибка [Semantic error] — ошибка программирования, возникающая из-за непонимания смысла, значения или действия той или иной конструкции программирования.

Сервер-посредник[Proxy server] — брандмауэр, в котором для преобразования IP-адресов всех авторизованных клиентов в IP-адреса, ассоциированные с брандмауэром, используется процесс, называемый трансляцией адресов (address translation).

Сертификат защиты [Protection certificate] — документ, удостоверяющий соответствие средств вычислительной техники или автоматизированной системы набору требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и/или распространение их как защищенных.

Сертификат соответствия в области защиты информации — документ, выдаваемый в соответствии с правилами сертификации, указывающий, что обеспечивается необходимая уверенность в том, что должным образом идентифицированные защищенные изделия, технические средства и способы защиты информации соответствуют конкретному стандарту или другому нормативному документу.

еще — действие органа по сертификации или другого независимого органа (лица) по его поручению, доказывающее, что обеспечивается необходимая уверенность в том, что должным образом идентифицированные защищенные изделия, технические средства и способы защиты информации соответствуют конкретному стандарту или другому нормативному документу.

Сертификация уровня защиты [Protection level certification] – процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных требований по защите.

Сетевая структура [network structure] — структура данных, представляющая множество, частично упорядоченное так, что по крайней мере для некоторых

элементов множества существует больше, чем один предыдущий элемент (ДСТУ 2874).

Сеть ЭВМ [Computer network] — совокупность сети передачи данных, взаимосвязанных ею ЭВМ и необходимых для реализации этой связи программного обеспечения и (или) технических средств, которая предназначена для организации распределенной обработки информации.

Сигнал — материальный носитель информации, представляющий любой физический процесс, параметры которого адекватно отображаютсообщение. По своей физической природе сигналы могут быть электрические, акустические, оптические, электромагнитные и т.д.

Сигнализация [Signaling] — 1) Передача сигналов. 2) Оповещение, предупреждение о чем-либо.

Сигнатура [Signature] — уникальная характеристика системы, которая может быть проверена. Примером сигнатуры может служить признак диска, используемый в качестве идентификационной метки диска-оригинала; этот признак не должен копироваться программным способом.

Система USENET — система обсуждения новостей на основе электронной почты, вначале разработанная для коммутируемых соединений, а сейчас использующая TCP/IP.

Система восстановления [Purification system] — комплекс программ и управляющих таблиц, предназначенных для поддержания целостности данных. Используется в банках данных и других автоматизированных системах.

Система замков и ключей [Locks and keys] — система защиты памяти, в которой сегментам памяти операционной системой присвоены идентификационные номера-замки, а зарегистрированным пользователям числовые коды-ключи. Это действие осуществляется привилегированным процессом в некоторой адресуемой области памяти, недоступной пользователю. Примером может служить слово состояния программы.

Система защиты данных [Security system] — комплекс аппаратных, программных криптографических средств, а также мероприятий, обеспечивающих защиту данных от случайного или преднамеренного разрушения, искажения или использования.

Система защиты информации — действующие в единой совокупности законодательные, организационные, технические и другие способы и средства, обеспечивающие защиту важной информации от всех выявленных угроз и возможных каналов утечки

еще — комплекс организационных и технических мероприятий по защите информации, проведенный на объекте с применением необходимых технических средств и способов в соответствии с концепцией, целью и замыслом защиты

еще — совокупность механизмов защиты, реализующих установленные правила, удовлетворяющие указанным требованиям.

Система защиты информации от несанкционированного доступа [System of protection from unauthorized access to information] — комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

Система защиты с полным перекрытием — система, в которой имеются средства защиты на каждый потенциально возможный путь проникновения к защищаемым данным.

Система защиты секретной информации [Secret information security system] — Комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах.

Система кодирования. [Coding system] — совокупность символов и правил кодирования; код.

Система обработки данных [data processing system] — система, состоящая из совокупности технических и программных средств, а также обслуживающего персонала, обеспечивающих обработку данных (ДСТУ 2874).

Система разграничения доступа [Security policy realization] — совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.

Система сертификации в области защиты информации — система, располагающая собственными правилами процедуры и управления для проведения сертификации соответствия в области защиты информации.

Система управления базами данных; СУБД [databases management system] — совокупность программных и языковых средств, обеспечивающих управление базами данных (ДСТУ 2874).

Системное прерывание [operation code trap] — состояние системы, аналогичное вызываемому обычным

сигналом прерывания, но синхронное с работой системы. Системное прерывание может быть вызвано множеством причин. Примерами ситуаций его возникновения являются попытка выполнения неправильной команды или попытка получения доступа к ресурсам другого пользователя в системе, поддерживающей защиту при работе в режиме нескольких пользователей

еще — некоторое значение, которое замещает обычную операционную часть машинной команды в определенной точке для того, чтобы вызвать прерывание во время выполнения этой машинной команды (ДСТУ 2873).

Системный аналитик [System analyst] — специалист, описывающий прикладные проблемы, определяющий спецификации системы, дающий рекомендации по изменениям оборудования, проектирующий процедуры обработки данных и методы верификации предполагаемых структур данных.

Системный журнал [Audit trail] — хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью инспекции конечного результата.

Системный ключ [System key] — ключ, обеспечивающий защиту систем ных средств от несанкционированного доступа.

Скремблер [Scrambler] — кодирующее устройство, используемое в цифровом канале, которое выдает случайную последовательность бит.

Скрытие [hiding] — способ технической защиты информации, состоящий в ухудшении условий обнаружения носителей информации и ее получения.

Скрытие объекта — способ защиты информации от технических разведок, предусматривающий устранение или ослабление технических демаскирующих признаков объекта защиты путем применения (использования) технических и организационных мероприятий по маскировке объекта.

Скрытый временной канал [Covert timing channel] — скрытый канал, в котором один процесс передает информацию другому посредством модуляции доступа к системным ресурсам (например, времени занятости центрального процессора) таким образом, что эта модуляция может распознаваться и детектироваться другим процессом.

Скрытый канал [Covert channel] — путь передачи информации, позволяющий двум взаимодействующим процессам обмениваться информацией таким способом, который нарушает системную политику безопасности.

Скрытый канал с памятью [Covert storage channel] — скрытый канал, обеспечивающий прямую или косвенную запись в пространство памяти одним процессом и чтение этой информации другим процессом. Скрытый канал с памятью обычно связан с использованием ресурсов ограниченного объема (например, секторов на диске), которые разделяются двумя субъектами с различными уровнями безопасности.

След [Footrprint] — в кодировании часть избыточного кода, которую можно использовать для выявления случаев нарушения авторского права.

След контроля [Audit trail] — записи о транзакциях, выполняемых в системе. Последовательность этих записей документирует ход обработки информации в системе, что позволяет проследить (провести трассировку) его: вперед от исходных транзакций до создаваемых в процессе их работы записей и/или отчетов или назад от конечных записей/отчетов до исходных транзакций. След контроля позволяет определить источники возникновения транзакций и последовательность их выполнения системой.

Служба безопасности [Security service] — совокупность должностных лиц и технических средств, обеспечивающая защиту систем связи и передаваемых данных.

Служба защиты — совокупность механизмов защиты, поддерживающих их файлов данных и организационных мер, которые помогают защитить ЛВС от конкретных угроз. Например, служба аутентификации и идентификации помогает защитить ЛВС от неавторизованного доступа к ЛВС , требуя чтобы пользователь идентифицировал себя , а также подтвердил истинность своего идентификатора. Средство защиты надежно настолько, насколько надежны механизмы, процедуры и т.д., которые составляют его.

Служебная тайна — охраняемые государством сведения в любой области науки, техники, производства и управления, разглашение которых может нанести ущерб интересам государства. К служебной тайне относится секретная информация с грифом "секретно".

Случайная антенна — електрическая цепь вспомогательного технического средства или системы

(ВТСС), способная принимать побочные электромагнитные излучения. Случайные антенны могут быть сосредоточенными и распределенными

Снятие замка — отмена процедуры защиты данных или программ, основанной на использовании замка защиты.

Собственник информации — субъект информационных отношений, обладающий юридическим правом владения, распоряжения и пользования информационным ресурсом. Юридическое право владения, распоряжения и пользования информационным ресурсом принадлежит лицам, получившим этот информационный ресурс по наследству. Авторам открытий, изобретений, научно — технических разработок, рационализаторских предложений и т.д. принадлежит право владения, распоряжения и пользования информацией, источником которой они являются.

Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами.

Содержание информации — конкретные сведения о данном объекте или явлении, определяющие совокупность элементов, сторон, связей, отношений между ними.

Сокрытие (утаивание) информации [Information hiding] — принцип разработки целостной структуры программы, согласно которому всякий компонент программы реализует или "упрятывает" единственное проектное решение.

Сообщение — информация, выраженная в определенной форме и предназначенная для передачи от источника информации к ее получателю с помощью сигналов различной физической природы. Сообщением могут быть телеграмма, фототелеграмма, речь, музыка, телевизионное изображение, данные на выходе ЭВМ и т.д., передаваемые по различным каналам связи, а также сигналы различной физической природы, исходящие от объектов защиты.

Сосредоточенная случайная антенна — случайная антенна, представляющая собой компактное техническое средство. К сосредоточенным случайным антеннам относятся телефонные аппараты, громкоговорители радиотрансляционной сети и другие компактные технические устройства и приспособления.

Сохранность данных [Data integrity] — способность информационной системы обеспечивать в течение своего жизненного цикла хранение данных в неискаженном виде и исключать их случайное уничтожение.

Социальная инженерия — обход системы безопасности информационной системы с помощью нетехнических мер(обмана и т.д.).

Спамминг [spamming] — посылка большого числа одинаковых сообщений в различные группы UNENET. Часто используется для организации дешевой рекламной компании, пирамид или просто для надоедания людям.

Специальная проверка — проверка технического средства обработки информации, осуществляемая с целью поиска и изъятия специальных электронных закладных устройств (аппаратных закладок).

Специальное техническое средство защиты — техническое средство защиты, разрабатываемое при создании объекта защиты и являющееся его составной частью. Конструкторская документация для изготовления специального технического средства защиты входит в документацию на объект защиты, а затраты на его разработку и производство включаются в стоимость разработки и изготовления (строительство) объекта защиты.

Специальное электронное закладное устройство (аппаратная закладка) — электронное устройство, несанкционированно и замаскированно установленное в техническом средстве обработки информации с целью обеспечить в нужный момент времени утечку информации, нарушение ее целостности или блокирование.

Специальные исследования — исследования, которые проводятся на объекте эксплуатации технических средств обработки информации с целью определения соответствия принятой системы защиты информации требованиям стандартов и других нормативных документов, а также для выработки соответствующих рекомендаций по доведению системы защиты до требуемого уровня. Специальные исследования проводятся с использованием необходимых средств и методов измерений. По результатам специсследований разрабатывается предписание на эксплуатацию. Специальные исследования могут предшествовать аттестации объекта комиссией или совмещаться с нею.

Специальные средства технической защиты информации [special purpuse facilities of information technical protection] — средства технической защиты информации, обеспечивающие самостоятельно или совме-

стно с другими средствами предотвращение утечки информации по нетиповым техническим

Список апробированной продукции [Evaluated Products List EPL] — список оборудования, аппаратуры и программного обеспечения, которое было оценено и признано соответствующим определенному классу, согласно стандарту Trusted Computer System Evaluation Criteria (TCSEC) — Оранжевая книга. EPL включен в Information System Security Products and Services Catalogue, издаваемый Агентством Национальной Безопасности (АНБ) США.

Список доступа [Access control list] — перечень пользователей сети, которым разрешен доступ к ресурсу ВОС, с указанием предоставленных прав доступа.

Список предпочтительной продукции [Preferred Products List (PPL)] — список коммерческой продукции (аппаратуры и оборудования), прошедшей испытания по программе TEMPEST и удовлетворяющей другим требованиям Агентства Национальной Безопасности (АНБ) США. PPL включен в Information System Security Products and Services Catalogue, издаваемый АНБ.

Способ защиты информации — прием (метод), используемый для организации защиты информации.

Способ защиты информации от технических разведок — преднамеренное воздействие на технический канал утечки информации или на объект защиты для достижения целей защиты от технических разведок. Основными способами защиты информации от технических разведок являются скрытие и дезинформации. Разновидностями дезинформации являются легендирование и имитации.

Средства восстановления [Restoring facility] — программы и процедуры, предназначенные для восстановления данных в случае их искажения или стирания.

Средства защиты от несанкционированного доступа [Protection facility] — программные, технические или программно-технические средства, предназначенные для предотвращения или существенного затруднения несанкционированного доступа.

Средства защиты программного обеспечения [Software protection device] — средства, обеспечивающие защиту программных средств отнесанкционированного доступа.

Средства криптографической защиты информации [Cryptographic information protection facility] — средства вычислительной техники, осуществляющие криптографическое преобразование информации для обеспечения ее безопасности.

Средства обеспечения информационных систем и их технологий — программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

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

Средства технической защиты информации общего назначения [general purpuse facilities of information technical protection] — средства технической защиты информации, обеспечивающие самостоятельно или совместно с другими средствами предотвращение утечки информации по типовым техническим каналам.

Средство вычислительной техники СВТ — техническое средство обработки информации, в котором информация представлена в цифровом коде. К средствам вычислительной техники относятся процессоры, каналы селективные и мультиплексные, внешние запоминающие устройства, устройства ввода и вывода данных, устройства непосредственной связи оператора с ЭВМ, устройства систем телеобработки данных, устройства повышения достоверности и т.д.

Средство защиты от технических разведок — техническое средство, предназначенное для устранения или ослабления демаскирующих признаков объекта защиты, создания ложных (имитирующих) признаков и воздействия на средства технической разведки с целью снижения их возможностей по получению разведывательной информации. По области применения различают специальные технические средства защиты и технические средства защиты общего назначения, по функциональному назначению — активные и пассивные технические средства защиты.

Средство криптографической защиты (информации) — аппаратно-программное средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Средство разграничения доступа — программно-аппаратное средство, обеспечивающее разграничение доступа субъектов к информационным ресурсам в соответствии с принятой моделью. Средствами разграничения доступа являются матрица доступа и метка секретности (конфиденциальности).

Средство технической разведки — аппаратура технической разведки, установленная и используемая на носителе.

Средства непосредственной защиты [Tamper resistance] — технические средства защиты, предназначенные для того, чтобы предотвратить или сделать крайне сложным любой доступ к устройству, используя для этих целей электрические связи.

Старение информации [Ageing of information] — свойство информации утрачивать со временем свою практическую ценность, обусловленное изменением состояния отображаемой ею предметной области.

Стационарный источник информации [Stationary source] — начиная с некоторого номера вероятностный механизм появления очередного символа на выходе источника не зависит от его номера.

Стратегия защиты [Security policy] — формальное определение критериев, особенно оперативных, которыми следует руководствоваться при обеспечении защиты системы от известных угроз.

Страховая форма защиты информации — защита информации, основанная на выдаче страховыми обществами гарантий субъектам информационных отношений по восполнению материального ущерба в случае утечки (рассекречивания) информации, ее модификации или физического уничтожения. Страховая форма защиты информации аналогична страхованию материального имущества и наиболее успешно может быть использована в частном секторе экономики.

Структурно-видовой демаскирующий признак объекта — технический демаскирующий признак, определяющий структуру и визуальные характеристики группового объекта: состав, количество и группировку единичных объектов, отражающие свойства их поверхностей, форму и геометрические размеры.

Субъект [Subject] — активная сущность (процесс, пользователь, устройство и т.д.), вызывающая образование информационного потока между объектами или изменения состояния системы.

еще — активный компонент системы, обычно представленный в виде пользователя, процесса или устройства, который может явиться причиной потока информации от объекта к объекту или изменения состояния системы. Обычно субъект представляется парой процесс — область.

Субъект безопасности [Security subject] — активная системная составляющая, к которой применяется методика безопасности.

Субъект доступа [Access subject] — лицо или процесс, осуществляющие доступ к информационному ресурсу с использованием штатных технических средств.

еще — лицо или процесс, действия которых регламентируются правилами разграничения доступа.

Субъект информационных отношений — физическое или юридическое лицо, обладающее определенным правом по отношению к информационному ресурсу. В зависимости от уровня полномочий субъект информационных отношений может быть источником, собственником, владельцем или пользователем информации.

Считыватель карт [Card reader] — устройство, предназначенное для считывания данных, записанных на карте, и их преобразования в двоичный код, пригодный для передачи с целью дальнейшей обработки. В устройствах считывания с магнитных карт имеется транспортировочный механизм, затягивающий карту в машину и перемещающий ее относительно считывающей головки. В некоторых устройствах перед считывающей головкой установлены специальные щетки для очистки карт. После считывания карты направление движения транспортировочного механизма меняется на противоположное и карта возвращается оператору. В устройствах, используемых в автоматах для выдачи наличными по кредитным карточкам, направление перемещения может не меняться, если карта и (или) указанный на ней идентификационный номер являются фальшивыми.

Считывать [Read] — воспринимать или восстанавливать (либо интерпретировать) данные, находящиеся в запоминающем устройстве или на входном носителе.

Т

Тестирование [testing] — применение тестов при проверке ЭВМ и ее программного обеспечения; выполнение действий, предусмотренных тестом.

Технико-экономическое обоснование защиты информации — определение оптимального объема организационных и технических мероприятий в составе системы защиты информации на объекте, необходимого для достижения цели защиты. При проведении исследований по технико-экономическому обоснованию следует исходить из того, что стоимость затрат на создание системы защиты информации на объекте не должна превышать стоимость защищаемой информации. В противном случае защита информации становится нецелесообразной.

Техническая дезинформация — способ защиты информации от технических разведок, предусматривающий введение технической разведки в заблуждение относительно истинного местоположения (дислокации) объекта защиты и его функционального назначения путем проведения комплекса мер по искажению технических демаскирующих признаков.

Техническая защита информации [technical protection of information] — защита информации при ее обработке техническими средствами, осуществляемая с использованием технических средств и способов защиты. К техническим средствам и способам защиты информации при ее обработке техническими средствами в общем случае относятся аппаратные, автономные (инженерные) и программные средства, а также криптографические методы.

еще — деятельность, направленная на обеспечение безопасности информации инженерно-техническими мерами.

Техническая разведка [technical intelligence] — получение сведений путем сбора и анализа информации техническими средствами.

Технический канал утечки информации [technical channel of information loss] — совокупность носителя информации, среды распространения полей или веществ и реального (или возможного) средства разведки, которая привела (может привести) к утечке информации.

Технический контроль эффективности защиты информации — контроль эффективности защиты информации с использованием технических средств (инструментальный контроль).

Техническое мероприятие по защите информации — мероприятие по защите информации, предусматривающее применение технических средств и способов защиты и реализацию технических решений.

Техническое решение по защите информации — техническое, планировочное, архитектурное или конструкторское решение по защите информации.

Техническое средство защиты информации — техническое средство, предназначенное для устранения или ослабления демаскирующих признаков объекта, создания ложных (имитирующих) признаков, а также для создания помех техническим средством доступа информации.

Техническое средство обработки информации (ТСОИ) — техническое средство, предназначенное для приема, хранения, поиска, преобразования, отображения и/или передачи информации по каналам связи. К техническим средствам обработки информации относятся средства вычислительной техники, средства и системы связи, средства записи, усиления и воспроизведения звука, переговорные и телевизионные устройства,средства изготовления и размножения документов, кинопроеционная аппаратура и другие технические средства, связанные с приемом, накоплением, хранением, поиском, преобразованием, отображением и/или передачей информации по каналам связи.

Техническое средство обработки разведывательной информации — техническое средство, предназначенное для сбора, сопоставления, логической увязки и обобщения разведданных и разведсведений для получения необходимой разведывательной нформации в соответствии с заданием потребителя.

Техническое устройство защиты [Physical protection device] — Устройство электронного или другого типа, предотвращающее возможность работы с программой лицам, не имеющим такого устройства.

Тип доступа [access type] — сущность права доступа к определенному устройству, программе, файлу и т.д. (обычно read, write, execute, append, modify, delete).

Тип записи (в базах данных) [record type (in databases)] — определенный класс записей, которые имеют одинаковые наборы полей данных (ДСТУ 2874).

Толерантность [Tolerance] — способность системы выдерживать изменения входных данных в определенном диапазоне без отказов и без нарушения правильности обработки.

Трафик [Trafic] — поток сообщений в сети передачи данных; рабочая нагрузка линии связи.

Требования (нормы) эффективности защиты информации — установленные (общепринятые) допустимые значения показателей эффективности защиты информации.

Троянский конь [Trojan horse] — специальная подпрограмма, которая разрешает действия, отличные от определенных в спецификации программы.

У

Убедительность защиты — принцип защиты, заключающийся в соответствии замысла защиты условиям обстановки, в которых он реализуется.

Угроза [threat] — угрозой может быть любое лицо , объект или событие, которое, в случае реализации, может потенциально стать причиной нанесения вреда ЛВС. Угрозы могут быть злонамеренными, такими, как умышленная модификация критической информации, или могут быть случайными, такими, как ошибки в вычислениях или случайное удаление файла. Угроза может быть также природным явлением, таким, как наводнение, ураган, молния и т.п. Непосредственный вред, вызванный угрозой, называется воздействием угрозы. В зависимости от своей направленности (нацеленности) различаются соответственно следующие основные виды угроз : утечка (рассекречивание) информации, нарушение ее целостности и блокирование

еще — любые обстоятельства или события, которые могут являться причиной нанесения ущерба системе в форме разрушения, раскрытия или модификации данных, и/или отказа в обслуживании.

еще — потенциальная возможность нарушения защиты от несанкционированного доступа.

Угроза безопасности информации — потенциальная возможность нарушения основных качественных характеристик (свойств) информации при ее обработке техническими средствами: секретности (конфиденциальности), целостности, доступности.

Угроза информации [information treat] — утечка или возможность на рушения целостности информации.

Умышленная (преднамеренная) ошибка [Intentional error] — ошибка, преднамеренно внесенная в программу или данные.

Уничтожение информации — случайное или умышленное стирание информации на ее носителях при обработке техническими средствами, в том числе хищение носителей и технических средств.

Управление базами данных [databases management] — процесс определения, создания, ведения баз данных, а также манипулирование ими (ДСТУ 2874).

Управление данными [data management] — процесс, обеспечивающий представление, накопление, хранение и использование данных, а также манипулирование ими (ДСТУ 2874).

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

еще — процесс ограничения доступа к ресурсам системы только разрешенным программам, процесса или другим системам (в сети).

Управление информационной безопасностью — способ обеспечения информационной безопасности путем использования механизмов обеспечения ЗИ.

Управление информационным потоком [Information flow control] — процедуры управления информационным потоком, удостоверяющие, что информация не может передаваться с верхних уровней безопасности на нижние (в соответствии с положениями модели Белла-Лападула, См. также определение скрытых каналов). Более общее определение контроля информационных потоков подразумевает процедуры управления, удостоверяющие, что информация не может передаваться по скрытым каналам (то есть в обход политики безопасности).

Управляемое разделение [Controlled sharing] — предоставление используемого ресурса двум или более использующим ресурсам с помощью некоторого механизма управления доступом.

Уровень (технической) защиты информации [(technical) protection information level] — совокупность методов и средств технической защиты информации, соответствующих нормируемым показателям.

Уровень безопасности [security level] — комбинация иерархической классификации (уровень доступа) и неиерархической категории, представляющих уровень критичности информации.

Уровень доступа [access level] — иерархическая часть метки уровня безопасности, используемая для идентификации критичности данных или прозрачности субъектов. Уровень доступа вместе с неиерархическими категориями составляет уровень безопасности.

Уровень полномочий субъекта доступа [Subject privilege] — совокупность прав доступа субъекта к информационному ресурсу.

Уровень прозрачности [Clearance] — максимальный уровень безопасности, доступ к которому разрешен данному субъекту правилами модели Белла-Лападула. Текущий уровень субъекта (уровень, на котором он в данный момент выполняет операции) может варьироваться от минимального до уровня прозрачности.

Услуга [service] — предоставление функциональных возможностей одного процессора другим процессорам (ДСТУ 2874).

Устройство выдачи сигнала тревоги — программно — аппаратное устройство, обеспечивающее выдачу звукового и/или светового сигнала на контрольный пост в случае попыток несанкционированного доступа.

Устройство повышения достоверности идентификации — программно-аппаратное устройство, обеспечивающее корректировку ошибок идентификации, переданных с удаленных терминалов по каналам связи. Для корректировки ошибок используются различные способы: обратная посылка сообщений на передающий конец для сравнения его с оригиналом, посылка одновременно с сообщением контрольных разрядов, использование избыточных кодов (код Хемминга, циклические коды) и т.д.

Устройство прерывания программы пользователя — программно-аппаратное устройство, обеспечивающее прерывание (блокирование) программы пользователя в случае попыток несанкционированного доступа.

Устройство регистрации доступа пользователей — программно-аппаратное устройство, обеспечивающее регистрацию пользователей при всех их обращениях к вычислительной системе с указанием номера терминала, даты и времени обращения.

Устройство стирания данных — программно-аппаратное устройство, обеспечивающее стирание оставшихся после обработки данных в ОЗУ путем записи нулей во все ячейки соответствующего блока памяти.

Устройство электромагнитного зашумления — широкополосный излучатель (генератор) электромагнитного шума,предназначенный для маскировки (подавления) информационного электромагнитного поля, создаваемого техническими средствами обработки информации, или наводок в токопроводящих коммуникациях, в заданной полосе частот.

Утечка (рассекречивание) информации — утрата информации , при ее обработке техническими средствами, свойства секретности (конфиденциальности) в результате несанкционированного ознакомления с нею или несанкционированного документирования (снятия копий).

Утечка информации [information loss] — неконтролируемое распространение информации, которое привело (может привести) к ее несанкционированному получению.

Уязвимость [Vulnerability] — свойство системы, которое может привести к нарушению ее защиты при наличии угрозы. Уязвимость может возникать случайно изза неадекватного проектирования или неполной отладки или может быть результатом злого умысла.

еще — слабость в системных средствах защиты, вызванная ошибками или слабостями в процедурах, проекте, реализации, внутреннем контроле системы, которая может быть использована для нарушения системной политики безопасности.

Уязвимые места — слабые места ЛВС, которые могут использоваться угрозой для своей реализации. Например, неавторизованный доступ (угроза) к ЛВС может быть осуществлен посторонним человеком, угадавшим очевидный пароль. Использовавшимся при этом уязвимым местом является плохой выбор пароля, сделанный пользователем. Уменьшение или ограничение уязвимых мест ЛВС может снизить или вообще устранить риск от угроз ЛВС. Например, средство, которое может помочь пользователям выбрать надежный пароль, сможет снизить вероятность того, что пользователи будут использовать слабые пароли и этим уменьшить угрозу несанкционированного доступа к ЛВС.

Ф

Фактор опасности — причина, обуславливающая появление угроз для безопасности информации при ее обработке техническими средствами. Основными факторами опасности для информации, обрабатываемой техническими средствами, являются: побочные электромагнитные излучения и наводки (ПЭМИН), несанкционированный доступ (НСД) к информации штатными техническими средствами, специальные электронные закладные устройства (аппаратные закладки) и внешние воздействия на информационный ресурс.

Фальсификация [spoofing] — использование различных технологий для обхода систем управления доступом на основе IP-адресов с помощью маскирования под другую систему, используя ее IP-адрес.

Физическая безопасность [physical security] — реализация физических барьеров и контрольных процедур, как превентивная или контрмера против физических угроз (взлома, кражи, террористического акта, а также пожара, наводнения и т.д.) ресурсам системы и критичной информации.

Физическое блокирование [Physical blocking] — блокирование, выполняемое в базах данных на физическом уровне.

Фиксация контроля средств защиты [Security audit trail] — совокупность сведений о состоянии средств защиты, накапливаемых во времени и предназначенных для упрощения управления средствами защиты.

Фиксированнопеременный код [Fixedtovariable code] — код, сопоставляющий векторам фиксированной длины кодовые последовательности переменной длины. В частности, вектором фиксированной длины на входе кодера может быть двоичная запись номера сообщения, порожденного источником. См. также *Код переменной длины*.

Форма существования информации — способ приспособления, выражения или представления информации, определяемый ее материальным носителем. Основными формами существования информации являются: человек, документ, изделие, работа (процесс), объект.

Формальная модель политики безопасности [Formal security policy model] — модель политики безопасности, выраженная точным, возможно математическим образом, включающим начальное состояние системы, способы перехода системы из одного состояния в другое и определение "безопасного" состояния системы.

еще — математически строгое описание политики безопасности. Подразумевает описание начального состояния системы, способы перехода системы из одного состояния в другое, а также определение безопасного состояния. Чтобы быть принятой как основа ДВБ (TCB), модель должна содержать формальное доказательство следующих положений: начальное состояние системы является безопасным; если все условия безопасности, определяемые моделью, выполнены, то все последующие состояния системы также будут безопасными. Примером формальной модели является модель Белла-Лападула.

Функциональные требования (спецификации функций безопасности) — подмножество функций ИС, относящихся к обеспечению ЗИ.

Функция скорость-погрешность [Ratedistortion function] — часто переводится как энтропия. Зависимость предельной скорости кодирования источника с критерием верности ("Coding with fidely criterion") от погрешности воспроизведения сообщений.

Х

Хакер [Hacker] — пользователь, который пытается вносить изменения в системное программное обеспечение, зачастую не имея на это право. Хакером можно назвать программиста, который создает более или менее полезные вспомогательные программы, обычно плохо документированные и иногда вызывающие нежелательные побочные результаты.

Хост-батистон [Batiston host] — компьютер-шлюз, на котором работает программное обеспечение брандмауэра и который устанавливается между внутренней и внешней сетями. Хост-бастионами являются шлюзы сеансового и прикладного уровня, а также брандмауэры экспертного уровня.

Ц

Целостность [Integrity] — состояние данных или компьютерной системы, в которой данные или программы используются установленным образом, обеспечивающим устойчивую работу системы; автоматическое восстановление в случае обнаружения системой потенциальной ошибки; автоматическое использование альтернативных компонентов вместо вышедших из строя. Примером является дублирование важных файлов с тем, чтобы в случае обнаружения ошибки или утери оригинального файла использовать его копию. Другим примером является поддержание двух и более путей доступа к устройству хранения.

Целостность базы данных [Database integrity] — состояние базы данных, когда все значения данных правильны в том смысле, что отражают состояние реального мира (в пределах заданных ограничений по точности и временной согласованности) и подчиняются правилам взаимной непротиворечивости. Поддержание целостности базы данных включает проверку целостности и восстановление из любого неправильного состояния, которое может быть обнаружено; это входит в функции администратора базы данных.

Целостность данных [Data integrity] — состояние, при котором данные, предоставленные в компьютере, в точности соответствуют данным в исходных документах. Свойство, относящееся к набору данных и означающее, что данные не могут быть изменены или разрушены без санкции на доступ. С сохранением целостности информации в базах данных связаны три аспекта: поддержание семантической целостности, управление параллельной обработкой данных, восстановление данных.

еще — свойство, при выполнении которого данные сохраняют заранее определенный вид и качество.

Целостность информации [Information Integrity] — свойство информации при ее обработке техническими средствами, обеспечивающее предотвращение ее несанкционированной модификации или несанкционированного уничтожения.

еще — способность средств вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

Целостность системы [system integrity] — качество системы, которым она обладает, если корректно выполняет все свои функции, свободна от намеренных или случайных несанкционированных манипуляций.

еще — состояние системы, в котором существует полная гарантия того, что при любых условиях компьютерная система базируется на логически завершенных аппаратных и программных средствах, обеспечивающих работу защитных механизмов, логическую корректность и достоверность операционной системы и целостность данных.

Цель защиты информации — заранее намеченный уровень защищенности информации, получаемый в результате реализации системы защиты на объекте.

Ценность информации [Information value] — свойство информации, определяемое ее пригодностью к практическому использованию в различных областях целенаправленной деятельности человека.

Цифровая подпись [Digital signature] — дополнительная информация, предоставляемая источником для обеспечения аутентификации. Последовательность данных, добавляемая к блоку данных или к результату его криптографического преобразования, которая позволяет получателю данных проверить источник и целостность блока данных, а также защиту от подлога или подделки.

Ч

Частная верификация [Partial verification] — доказательство правильности программ, учитывающее основные, но не все возможные факторы.

Частная информация [Private data] — личная информация, данные, доступные только их владельцу.

Человек — форма существования информации, обусловленная свойством человека накапливать и хранить в своем сознании (памяти) смысловую информацию, а при необходимости выдавать ее другому человеку или техническоу устройству. Выдача человеком информации происходит устно при разговоре, письменно в виде документа или путем передачи изделий различного назначения.

Червь [Worm] — программа, внедряемая в систему, часто злонамеренно, и прерывающая ход обработки информации в системе. В отличие от вирусов червь обычно не искажает файлы данных и программы. Обычно червь выполняется, оставаясь необнаруженным, и затем самоуничтожается.

Ш

Шифр [Cipher] — совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключа.

еще — криптографический прием, связанный с применением некоторого алгоритма преобразования символов (букв и цифр) исходного (незашифрованного) текста в зашифрованный. Ср. код.

Шифратор [Encoder, encipher] — 1) Устройство, изменяющее характер представления информации за счет изменения принципов кодирования. 2) Блок ЭВМ, выполняющий преобразование входных сигналов.

Шифрование (информации) — процесс зашифрования или расшифрования информации.

еще — криптографическое преобразование данных для получения шифрованного текста.

Шифрование методом РША (Ривеста Шамира Адлемана) [Rsa Encryption] — метод шифрования, предложенный Ривестом, Шамиром и Адлеманом, при котором ключ, используемый для шифрования, не совпадает с ключом для дешифрирования (последний должен быть известен получателю); по этой причине данный метод относят к методам шифрования с открытым ключом.

Шифрование с открытым ключом [Public key cryptography] — криптографический метод, в котором используются раздельные ключи для шифрования и дешифрования.

Шлюз прикладного уровня [Application-level gateway] — исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Шлюз фильтрует все входящие и исходящие пакеты на прикладном уровне модели OSI. Связанные с приложениями программы-посредники перенаправляют через шлюз информацию, генерируемую конкретными сервисами TCP/IP.

Шлюз сеансового уровня [Circuit-level gateway] — исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Он принимает запрос доверенного клиента на определенные услуги и, после проверки допустимости запрошенного сеанса, устанавливает соединение с внешним хостом.

После этого шлюз просто копирует пакеты в обоих направлениях, не осуществляя их фильтрации.

Штатное техническое средство (информационного доступа) — техническое средство, входящее в комплект средств вычислительной техники, установленный на объекте, или другое СВТ, используемое для проведения диалога с вычислительной системой и осуществления доступа к информационному ресурсу.

Э

Экранирующее сооружение — объемно-пространственное или плоское сооружение, предназначенное для отражения и поглащения излучений объекта защиты.

Эксперт-аудитор в области защиты информации — лицо, аттестованное на право проведения одного или нескольких видов работ в области сертификациии защищенных изделий, технических средств и способов защиты информации.

Экспертиза системы защиты информации — оценка соответствия представленных проектных материалов по защите информации (на объекте) поставленной цели, требованиям стандартов и других нормативных документов.

Экспертная система [Expert system] — комплекс программных средств, в основу которого положена интерпретация правил, аккумулирующих знания экспертов по определенной специальности.

Электрический фильтр — электротехническое развязывающее устройство в цепях электроснабжения, линиях связи и других токопроводящих коммуникациях, предназначенное для пропускания определенного диапозона частот электрических колебаний.

Электроакустический канал утечки акустической (речевой) информации — канал утечки акустической (речевой) информации, обусловленный преобразованием акустических колебаний в электрические и обратно и распространение этих колебаний в различных присущих им средах.

Электроакустический преобразователь — устройство, предназначенное для преобразования акустических колебаний в электрические и обратно.

Электромагнитная наводка — индуцирование электрических сигналов в цепях вспомогательных технических средств и систем (ВТСС) за счет побочных электромагнитных излучений технических средств обработки информации, приводящее к утечке информации по токопроводящим коммуникациям за пределы контролируемой зоны.

Электромагнитная совместимость — условия совместного использования радиоэлектронных средств, при которых взаимные помехи не влияют на их работоспособность.

Энтропия [Entrophy] — в теории информации мера неопределенности состояния объекта или некоторой ситуации (случайной величины) с конечным числом исходов. Понятие энтропии введено Шенноном. Используется для определения количества информации в сообщении. Так, количество информации при равновероятности всех значений сообщения определяется по формуле H=k*log m, где H энтропия, k число знаков в сообщении, m число знаков в алфавите источника.

Эффективность защиты информации [information techmical protection efficiency] — степень соответствия достигнутого уровня защищенности информации поставленной цели.

еще — показатель, характеризующий уровень технической защиты информации.

Я

Ядро безопасности [security kernel] — программные и аппаратные элементы ДВБ (TCB), реализующие концепцию монитора ссылок. Они должны разделять все попытки доступа субъектов к объектам, быть защищенным от модификации и проверены на корректное выполнение своих функций.

Ядро защиты [Security kernel] — технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа.

Язык Java — новый язык программирования, разработанный Sun Microsystems, Inc. Он может использоваться как обычный язык программирования для разработки сетевых приложений. Кроме того, он используется для написания небольших приложений, называемых апплетами. Среда для выполнения Java-апплетов должна быть безопасной, то есть апплет не должен иметь возможности модифицировать что-либо вне WWW-браузера.

Язык администрирования базы данных [database administration language] — искусственный язык для описания действий, связанных с администрированием базы данных (ДСТУ 2874).

Язык базы данных [database language] — искусственный язык для описания процессов создания, ведения и использования баз данных(ДСТУ 2874).

Язык гипертекстовой разметки документов [HTML] — используется для создания Web-страниц.

Язык запросов [query language] — искусственный язык для описания запросов, поиска данных в базах данных и действий над запросами (ДСТУ 2874).