Центр стратегических оценок и прогнозов

www.csef.ru

Информационная война и защита информации

Словарь основных терминов и определений

Москва - 2011

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современный этап развития общества характеризуется возрастающей ролью информации во всех сферах жизни и деятельности человека. Сегодня информационная сфера, являясь системообразующим фактором современного общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности государств. Во многом целостность современного мира как сообщества обеспечивается, в том числе, за счет интенсивного информационного обмена. Приостановка глобальных информационных потоков даже на короткое время способно привести к не меньшему кризису, чем разрыв межгосударственных экономических отношений. Как отмечается в Доктрине информационной безопасности, национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе развития технического прогресса эта зависимость будет возрастать.

Переход информации в разряд важнейших ресурсов человечества вызывает к жизни и проблему борьбы за обладание этим ресурсом. Информационный ресурс является весьма специфической составляющей в совокупности ресурсов развития государства. Его объекты и объединяющая их информационная инфраструктура имеют своеобразные особые пространственно-временные характеристики, не ограничивающиеся пределами национальной территории. Кроме того, сама информация обладает уникальными свойствами делимости и воспроизводимости. Все эти факторы заметно сказываются на общей оценке потенциала того или иного геополитического субъекта, на его способности к устойчивому развитию, на возможности воздействовать на него извне, восприимчивости к скрытому перераспределению информационного ресурса противника силами, средствами и способами информационной борьбы. Считается, что ведущееся вокруг информационного ресурса соперничество, борьба за обладание этим ресурсом, достижения и удержания информационного превосходства сегодня занимает значительное место в геополитической конкуренции развитых стран.

В настоящее время в борьбе за сферы экономического и политического влияния в международных отношениях акцент с применения военной силы все больше смещается на использование более скрытных и гибких форм, одной из которых является контроль и управление информационными ресурсами государств. Информационное воздействие в этой связи рассматривается как новый вид оружия, которое в определенной степени является не менее эффективным средством воздействия, чем традиционное вооружение и военная техника.

Многие признают тот факт, что в современном мире (а тем более в будущем) статус «великой державы» будет определяться способностью к развитию, к лидерству в приоритетных сферах знаний, информатике, технологиях и повседневному влиянию на жизнь миллионов людей во всем мире через потребляемые ими продукты, товары, услуги, культуру.

Российская Федерация, обладающая значительным военным и экономическим потенциалом и представляющая для стран Запада серьезное препятствие на пути к мировому господству, является объектом пристального внимания спецслужб иностранных государств, занимающихся информационным противоборством.

В настоящем справочнике предпринята попытка обобщить ряд источников и сформировать единый взгляд на предметную область, очерченную словосочетаниями «информационная война» и «защита информации».

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

АБОНЕНТ - пользователь, имеющий право доступа к системе обработки или передачи информации.

АБСТРАГИРОВАНИЕ - логическая операция анализа информации, процесс выделения отдельных, наиболее интересных в данный момент признаков, свойств и отношений изучаемого предмета или явления и отделение их от других признаков, свойств, отношений этого предмета, которые не способствуют его изучению, а часто даже затрудняют это изучение.

АВАРИЯ - происшествие, в результате которого повреждена или разрушена техника обработки информации или средства ее защиты, приведшая к потере информации или появлению возможности несанкционированного доступа к ней.

АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА - информационная система, реализованная с использованием средств вычислительной техники и связи.

АВТОМАТИЗИРОВАННЫЙ КОМАНДНЫЙ ПУНКТ ЧАСТИ РАДИОЭЛЕКТРОННОЙ БОРЬБЫ - стационарный или подвижный командный пункт части РЭБ, оснащенный автоматизированными рабочими местами должностных лиц боевого расчета.

АВТОРИЗАЦИЯ - 1) представление субъекту некоторых прав доступа к информации; 2) определение типов действий, разрешенных данному пользователю. Обычно разрешение находится в контексте установления подлинности. Как только подтверждена подлинность пользователя, ему могут быть разрешены различные типы доступа или деятельности в соответствии с его полномочиями.

АГИТАЦИЯ - форма информационно-психологического воздействия на эмоциональную сферу объектов (групп объектов) с целью достижения определенного психологического состояния, побуждающего к активным, конкретным действиям.

АДМИНИСТРАТОР ЗАЩИТЫ - субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

АДМИНИСТРАТОР ИНФОРМАЦИОННОЙ СИСТЕМЫ - человек, обслуживающий систему управления информацией или малую многопользовательскую вычислительную систему.

АКТИВНАЯ ПРЕДНАМЕРЕННАЯ РАДИОЭЛЕКТРОННАЯ ПОМЕХА (АКТИВНАЯ ПОМЕХА) - радиоэлектронная помеха, создаваемая непосредственно излучением источника помех.

АКТИВНАЯ УГРОЗА - угроза преднамеренного несанкционированного изменения состояния системы: 1) примерами активных угроз, относящихся к защите информации, могут служить модификация сообщений, дублирование сообщений, вставка ложных сообщений, маскировка какого-либо логического объекта под санкционированный логический объект и отклонение услуги; 2) активные угрозы системе означают изменение информации, содержащейся в системе, либо изменение состояния или работы системы. Примером активной угрозы служит умышленное изменение таблиц маршрутизации системы неполномочным пользователем.

АКТИВНОЕ СРЕДСТВО ЗАЩИТЫ - средство, обеспечивающее создание активных помех средствам технической разведки (промышленного шпионажа) или разрушение нормального функционирования этих средств.

АКУСТИЧЕСКАЯ ИНФОРМАЦИЯ - информация, носителями которой являются акустические сигналы.

АКУСТИЧЕСКИЕ ПОМЕХИ - непоражающие акустические излучения, которые ухудшают качество

функционирования РЭС, работающих на принципе приема, усиления и преобразования акустических волн. Акустические помехи, применяемые в водной среде, называются гидроакустическими.

АКУСТИЧЕСКИЙ СИГНАЛ - возмущение упругой среды, проявляющееся в возникновении акустических колебаний различной формы и длительности.

АКУСТИЧЕСКОЕ ПОДАВЛЕНИЕ - преднамеренное подавляющее или маскирующее воздействие акустической энергией на акустические средства. Акустическое подавление в водной среде называется гидроакустическим подавлением.

АНАЛИЗ ПРОЦЕДУР ЗАЩИТЫ - независимый просмотр и анализ системных записей и активностей с целью проверки их адекватности системным управляющим функциям для обеспечения соответствия с принятой стратегией защиты и операционными процедурами, обнаружения пробелов в защите и выдачи рекомендаций по любым указанным изменениям в управлении, стратегии и процедурах.

АНТИВИРУСНАЯ ПРОГРАММА - компьютерная программа, обнаруживающая и удаляющая вирусы.

АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ - механические, электротехнические, электронные, оптические, лазерные, радио-, радиотехнические, радиолокационные и другие устройства, системы и сооружения, предназначенные для защиты информации от несанкционированною доступа, копирования, кражи или модификации Аппаратура засекречивания специальные технические устройства для автоматического шифрования (дешифрования) телефонных и телеграфных переговоров (сообщении).

АППАРАТУРА ПЕРЕДАЧИ ДАННЫХ, СРЕДСТВА - обеспечивающие связь между ЭВМ в системах телеобработки данных.

АППАРАТУРА ТЕХНИЧЕСКОЙ РАЗВЕДКИ - совокупность технических устройств обнаружения, приема, регистрации, измерения и анализа, предназначенных для получения данных об объекте.

АТАКА АКТИВНАЯ - форма *атаки информационной*, в результате которого фактически изменяются или уничтожаются хранимые или обрабатываемые в нем данные или другие элементы ресурса.

АТАКА АСИНХРОННАЯ - форма *атаки информационной*, при которой используются преимущества динамических действий системы, особенно способность управлять выбором времени исполнения тех или иных действий.

АТАКА ИНФОРМАЦИОННАЯ - попытка предпринять *воздействия несанкционированные* на информационное пространство противника с целью его модификации в своих интересах.

АТАКА КОНТРОЛИРУЕМАЯ - форма *атаки информационной*, направленной на основной поток сообщений в сети Ethernet (например, контролируя пачки, проходящие через маршрутизатор) и изменение порядка дальнейшего движения для сообщений определенного вида или с определенными признаками (например, содержащих конкретный пароль). Этот процесс может быть выполнен автоматическими специально встраиваемыми средствами или с использованием программ-пересмешников.

АТАКА ПАССИВНАЯ - форма *атаки информационной*, при которой снимается ограничение на доступ к данным (см.: доступ ограниченный) или изменяется порядок контроля доступа к данным.

АУТЕНТИФИКАЦИЯ - 1) проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности; 2) положительная процедура установления пользователя, устройства или другого активного элемента в системе информационной по его заявленным полномочиями и паролю, иногда с использованием других, в частности,

биометрических характеристик или предъявляемых электронных ключей.

АУТЕНТИФИКАЦИЯ ИНФОРМАЦИИ - установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от ее источника.

АУТЕНТИФИКАЦИЯ ОТПРАВИТЕЛЯ ДАННЫХ - подтверждение того, что отправитель полученных данных соответствует заявленному.

БАЗА ДАННЫХ - 1) объективная форма представления и организации совокупности данных (статей, расчетов и так далее), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ; 2) совокупность организованных, взаимосвязанных данных на машиночитаемых носителях.

БАНК ДАННЫХ - организационно-техническая система, включающая в себя одну или несколько баз данных и управление ими.

БЕЗОПАСНОСТИ КРИТЕРИИ - показатели, качественно и количественно характеризующие достигнутый уровень той или иной системы безопасности.

Критерии военно-политической безопасности государства позволяют оценивать его социально-политический, экономический и военный потенциалы, их соответствие реальным и прогнозным внешним военным угрозам, оценивать и сопоставлять численные соотношения сил и средств вооруженных сил государств - вероятных противников и союзников,

Критерии военно-экономической безопасности государства обеспечивают возможность оценки уровня мирового и собственного военного производства, военного производства вероятных противников, способность обеспечивать население и вооруженные силы всем необходимым в мирное и особенно в военное время, а также восполнять в случае войны неизбежные потери.

Все более заметное место в процессе военных исследованиях стали занимать критерии оценки экологической и информационной защищенности государства и сопредельных с ним стран.

БЕЗОПАСНОСТИ МОДЕЛЬ - количественно-качественное описание возможного варианта построения системы безопасности, предусматривающее определение ее целей и задач, оценку возможных угроз и механизмов повышения защищенности системы от этих угроз.

Так, в модели военной безопасности отражается характер отношений между государствами, уровень их военной и военно-экономической мощи, вероятная расстановка военно-политических сил и динамика их развития, дается описание структуры органов и механизмов обеспечения военной безопасности, направленности совместных и самостоятельных усилий стран по организации национальной и коллективной обороны, способов совместных и односторонних действий по предупреждению войны и устранению других угроз.

Различают политические, военные, экономические, информационные, экологические и другие модели безопасности. Между ними формируются связи, обусловливающие их согласованное функционирование. На основе моделей оценивается эффективность тех или иных систем безопасности, анализируются целесообразность и последствия тех или иных решений, которые могут приниматься в области анализируемой безопасности.
Модели используются как инструмент исследований, анализа и обоснования практических рекомендаций руководящим органам государства.

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ - 1) защита информации от случайного или преднамеренного доступа лиц, не имеющих на это права, ее получения, раскрытия, модификации или разрушения. Реализация требований и правил по защите информации, поддержанию информационных систем в защищенном состоянии, эксплуатация специальных технических и программно-математических средств защиты и обеспечение организационных и инженерно-технических мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляется службами безопасности информации; 2) состояние защищенности информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п..

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННАЯ - 1) состояние защищенности основных интересов личности, общества и государства в пространстве информационном, включая инфраструктуру информационно-телекоммуникационную и собственно информацию в отношении таких ее свойств, как целостность, объективность, доступность и конфиденциальность; 2) совокупное состояние: пространства информационного, при котором обеспечивается его формирование и развитие в интересах граждан, организаций и государства; инфраструктуры информационной, при котором информация используется строго по назначению и не оказывает негативного воздействия на систему (объект) при ее использовании; информации, при котором исключается или существенно затрудняется нарушение таких ее свойств, как конфиденциальность, целостность и доступность; 3) защищенность информационной среды личности, общества и государства от преднамеренных и непреднамеренных угроз и воздействий; 3) проведение правовых, организационных и инженерно-технических мероприятий при формировании и использовании информационных технологий, инфраструктуры и информационных ресурсов, защите информации высокой значимости и прав субъектов, участвующих в информационной деятельности.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОЙ СЕТИ - меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов. Включает защиту оборудования, программного обеспечения, данных.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ РЕСУРСОВ - состояние защищенности ИР от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ - состояние защищенности информации и ресурсов ИТ от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способность ИТ выполнять предписанные функции без нанесения неприемлемого ущерба субъектам информационных отношений.

БЕЗОПАСНОСТЬ НАУЧНО-ТЕХНОЛОГИЧЕСКАЯ - состояние защищенности научно-технического и технологического потенциала от уязвимости, застоя, разрушения и деградации с целью обеспечения суверенитета, социально-экономического развития государства и его национальной безопасности, повышения конкурентоспособности отечественной наукоемкой продукции.

Научно-технологическая безопасность государства предполагает:

- воспроизводство национального научно-технического, технологического и производственного потенциала;
- развитие приоритетных направлений научных исследований и технических разработок, обеспечивающих конкурентоспособность национальной экономики;
- обеспечение режима секретности и охраны на объектах стратегической важности, производствах повышенной опасности, в научно-исследовательских организациях и на предприятиях, работа которых составляет предмет государственной тайны;
- экспортный контроль за распространением технологий и научных разработок;
- защита прав интеллектуальной собственности в сферах внешнеэкономической деятельности и научно-технического сотрудничества;
- разведывательная и контрразведывательная деятельность в сфере технологий и научных разработок, имеющих стратегическое значение.

БЕЗОПАСНОСТЬ СВЯЗИ - 1) способность связи противостоять несанкционированному получению или изменению передаваемой информации; 2) обеспечение защиты, являющееся результатом всех мер, направленных на недопущение лиц, не имеющих на то разрешения, к ценной информации, которая может быть извлечена при обладании и изучении сообщений систем связи или на введение в заблуждение лиц, не имеющих допуска, в их интерпретировании результатов такого обладания и изучения. Безопасность связи включает в себя обеспечение безопасности закрытой связи, безопасность радиопередач, обеспечение безопасности работы средств связи и электронного оборудования и обеспечение физической безопасности материалов и информации по вопросам безопасности связи.

Обеспечение безопасности закрытой связи, компонент обеспечения безопасности связи, являющийся результатом наличия технически совершенных криптосистем и их правильного использования.

Безопасность радиопередач, компонент обеспечения безопасности связи, являющийся результатом всех мер, направленных на защиту радиопередач от перехвата и использования в других целях, кроме криптоанализа.

Обеспечение безопасности средств связи и электронного оборудования, компонент обеспечения безопасности связи, являющийся результатом всех мер, предпринимаемых, чтобы не допустить лиц, не имеющих на то разрешения, к ценной информации, которая может быть извлечена из перехвата и анализа излучений шифровального оборудования и систем дальней связи.

Физическая безопасность связи, компонент обеспечения безопасности связи, являющийся результатом всех физических мер, необходимых для защиты секретного оборудования, материалов и документов от доступа к ним или наблюдения за ними со стороны лиц, не имеющих на то разрешение.

БЛОКИРОВАНИЕ ДОСТУПА К ИНФОРМАЦИИ - прекращение или затруднение доступа законных пользователей к информации.

БОЕПРИПАС ПРЕДНАМЕРЕННЫХ ПОМЕХ (БОЕПРИПАС ПОМЕХ) - боеприпас, снаряженный средствами радиоэлектронного подавления.

БОМБА ЛОГИЧЕСКАЯ - обобщающий термин деструктивных программных комплексов, резидентно находящихся на компьютере «жертвы» и активирующихся по определенному логическому условию (например, достижение определенной даты или набора определенных состояний системы). Наиболее известным и распространенным является срабатывание логической бомбы на заранее заданный контекст (ключевое слово). Может быть самостоятельной программой или фрагментом кода, распространяемым программистами или производителем некоторого программного продукта (пакета программ). Используется для инициирования вирусной или иного рода программной атаки на компьютерную систему. Механизм разрушающего воздействия может быть сколь угодно различным.

БОРЬБА С СИСТЕМАМИ БОЕВОГО УПРАВЛЕНИЯ - мероприятия и действия, проводимые войсками (силами) по выявлению и дезорганизации систем управления, связи и разведки противника в целях снижения способности руководства противника эффективно управлять вооруженными силами. Концепция борьбы с СБУ выдвинута в США в конце 70-х годов в дополнение к понятию «радиоэлектронная борьба».

Целью борьбы с СБУ является поражение объектов, оборудование, средств связи, автоматизации, а также радиоэлектронное подавление систем управления, связи и разведки для их дезорганизации и снижения возможностей противника эффективно управлять войсками (силами) и оружием. В операции (бою) это достигается проведением следующих действий: детальная разведка указанных систем, выбор первоочередных объектов и их поражение артиллерийским огнем, ударами авиации и разведывательно-ударными комплексами; захват командных пунктов, узлов связи, центров обработки разведывательных данных и радиоэлектронных объектов; радиоэлектронным подавлением СБУ; введение противника в заблуждение путем использования его РЭС разведки и радиолиний связи; организация утечки заведомо ложной информации. Наряду с этим предусматривается проведение мероприятий по психологической борьбе.

Кроме систематических действий по дезорганизации СБУ, планируются специальные операции с привлечением разведывательно-диверсионных подразделений.

Технической основой реализации концепции борьбы с СБУ считается применение высокоточного оружия, систем радиоэлектронного подавления и разведки, а также других информационных средств, интегральная совокупность которых по опыту локальных конфликтов из категории обеспечивающих средств была переведена МО США в категорию оружия (см. информационное оружие ТВД).

ВЕДОМСТВЕННЫЕ СЕТИ СВЯЗИ - сети электросвязи министерств и иных федеральных органов исполнительной власти, создаваемые для удовлетворения производственных и специальных нужд, имеющие выход на сеть связи общего пользования.

ВЕРИФИКАЦИЯ - процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие.

ВЗАИМОУВЯЗАННАЯ СЕТЬ СВЯЗИ РОССИЙСКОЙ ФЕДЕРАЦИИ - комплекс технологически сопряженных сетей электросвязи на территории РФ, обеспеченный общим централизованным управлением.

ВЗЛАМЫВАНИЕ ПАРОЛЯ - техника (способ) тайно получать доступ к информационной системе (сети), в которой нападавшие пробуют угадать (определить) или украсть пароли. Пользователи часто выбирают слабый пароль. Два главных источника слабости в паролях, легко предполагаемые пароли, основанные на знании пользователя (например, девичья фамилия жены) и пароли, которые являются восприимчивыми к раскрытию с использованием словаря как источника предположений. Эта техника была легко автоматизирована хакерами, компьютеры могут очень эффективно и систематически делать предположение. Например, если пароль, слово словаря, компьютер может быстро посмотреть все возможности.

ВИДЫ МЕХАНИЗМОВ ЗАЩИТЫ - некоторыми видами механизмов защиты являются:
методы криптографирования и шифрование, аспекты административного управления ключами, механизмы цифровой подписи, механизмы управления доступом, механизмы целостности данных, механизмы обмена информацией аутентификации, механизмы заполнения трафика, механизм управления маршрутизацией, механизм нотаризации, физическая или персональная защита, надежное аппаратное/программное обеспечение.

ВИРТУАЛЬНОЕ ПОЛЕ БОЯ - применяется в военном контексте как эфир, занятый импульсами коммуникаций, базами данных, компьютерными сообщениями. В этом использовании, синонимичен киберсреде, киберпространству, инфосфере.

ВИРУС КОМПЬЮТЕРНЫЙ - 1) вредоносная программа, способная создавать свои копии или другие вредоносные программы и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия; 2) родовое наименование большого числа вредоносных программ, главной отличительной чертой которых является способность к «саморазмножению» или «самораспространению» при определенных условиях. Точного определения вируса к. нет до сих пор и вряд ли оно появится в обозримом будущем. Вирус компьютерный обычно «инфицирует» компьютерные файлы (исполняемые программы, файлы документов или другие выполняемые объекты), вставляя в них собственные копии. Это обычно делается так, что копии вируса будут выполняться, когда файл загружается в память компьютера, инфицируя при этом еще и другие файлы и т.д. Есть компьютерные вирусы, которые не инфицируют никаких файлов, но обладают способностью к распространению и выполнению злоумышленных действий, используя тонкие особенности устройства ПЭВМ, операционных систем, файловых систем и сетевых протоколов. Вирусы часто приводят к повреждению или полной утрате информации пользователя. Количество известных компьютерных вирусов превышает 15000. Деятельность по написанию и распространению компьютерных вирусов во многих странах преследуется по закону; 3) небольшая, достаточно сложная, тщательно составленная и опасная программа, которая может самостоятельно размножаться, переносить себя на диски, прикрепляться к чужим программам и передаваться по информационным сетям. Обычно создается для нарушения работы компьютера различными способами — от «безобидной» выдачи какого-либо сообщения до стирания, разрушения файлов. Выявление «вирусов» и «лечение» инфицированных файлов осуществляется различными методами, в том числе специальными антивирусными программами.

ВМЕШАТЕЛЬСТВО В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И ИНФОРМАЦИОННЫЕ РЕСУРСЫ НЕСАНКЦИОНИРОВАННОЕ - вмешательство в процессы сбора, обработки, накопления, хранения, отображения, поиска, распространения и использования информации с целью нарушения нормального функционирования систем или нарушение

целостности, конфиденциальности и доступности информационных и телекоммуникационных ресурсов.

ВНЕШНИЕ ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов РФ в информационной сфере;
- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

ВНУТРЕННИЕ ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти по формированию и реализации единой государственной политики в области обеспечения ИБ;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности РФ;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения ИБ;
- недостаточная активность федеральных органов государственной власти в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации органов государственной власти, местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

ВНУТРИПРОИЗВОДСТВЕННЫЕ И ТЕХНОЛОГИЧЕСКИЕ СЕТИ СВЯЗИ - сети электросвязи федеральных органов исполнительной власти, а также предприятий, учреждений и организаций, создаваемые для управления внутрипроизводственной деятельностью и технологическими процессами, не имеющие выхода на сеть связи общего пользования.

ВНУШАЕМОСТЬ (СУГГЕТИВНОСТЬ) - относительно устойчивое состояние психики, заключающееся в податливости психики внушающему воздействию, базирующееся на психических особенностях объекта внушения, но окончательно устанавливаемое в процессе его взаимодействия с субъектом внушения и своим социальным окружением.

ВНУШЕНИЕ - метод психологического воздействия в психологических операциях, рассматриваемый как целенаправленное и сознательно организуемое воздействие на объект (группу объектов), осуществляемое на основе некритического восприятия информации с целью вызова определенного поведения объекта внушающего' воздействия, характеризующееся глубиной эмоционального воздействия, апелляцией к чувствам, проводимый в соответствии с целями психологической операции и использующий как вербальные, так и невербальные средства.

ВОЗДЕЙСТВИЕ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЕ - применение информационно-психологических способов и средств на психику человека с целью ее модификации в нужном для воздействующей стороны направлении.

ВОЗДЕЙСТВИЕ ИНФОРМАЦИОННО-ЭНЕРГЕТИЧЕСКОЕ - воздействие на биосистемы, и прежде всего на человека, физических полей различной природы, модулированных семантическими (смысловыми) сигналами, воспринимаемое биологическими организмами, а также средой их обитания в форме сигналов, сообщений, сведений, образов (те в виде некоторой информации).

ВОЗДЕЙСТВИЕ НА ИНФОРМАЦИОННОЕ ПРОСТРАНСТВО СИЛОВОЕ - нарушение с использованием оружия информационного нормального (установленного законными собственниками, владельцами и пользователями) функционирования инфраструктуры общества информационной, правил формирования, хранения и распространения информации и информационных ресурсов.

ВОЗДЕЙСТВИЕ НА ИНФОРМАЦИЮ - согласованные по целям, задачам, месту и времени мероприятия, направленные на перехват (съем), искажение или уничтожение сведений и сообщений в процессе их сбора, обработки, хранения или передачи по информационным каналам систем управления и связи.

ВОЗДЕЙСТВИЕ ПУТЕМ ПРОВЕДЕНИЯ МАТЕРИАЛЬНЫХ АКЦИЙ - форма информационно-психологического воздействия, основанная на формировании положительных эмоциональных состояний у объекта воздействия на основе позитивной оценки осуществляемых субъектом действий по отношению к объекту (раздача гуманитарной помощи, строительство и восстановление разрушенной в результате боевых действий инфраструктуры, объектов социального назначения и т.п.), это убеждение не словом, а делом.

ВОЗДЕЙСТВИЕ ЧЕРЕЗ ИНФОРМАЦИОННЫЕ КОМПЬЮТЕРНЫЕ СЕТИ - форма информационно-психологического воздействия, основанная на использовании региональных и глобальных коммуникационных линий компьютерной связи в качестве средства передачи специально подготовленного материала.

ВОЙНА ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ (ПСИХОЛОГИЧЕСКАЯ) - широкомасштабное применение способов и средств информационного воздействия на психику личного состава войск и населения противника в интересах достижения воздействующей стороной политических, дипломатических, военных, экономических и других целей.

Война информационно-психологическая направлена на разрушение основ национального самосознания и типа жизнеустройства государства противоборствующей стороны, на подрыв морально-политического и психологического состояния населения и личного состава войск противника, а также на защиту от таких действий со стороны врага. Может вестись как в военное, так и в мирное время. В ходе войны приобретает большой размах и новые формы.

Основу психологической войны в современных условиях может составлять подготовка и проведение крупных психологических и идеологических акций, диверсий, операций и стратегических действий по специально разработанным планам с определенными целями,

главными из которых могут быть:

- ослабление обороноспособности противника, подрыв боеготовности и боеспособности его войск, снижение боевой устойчивости личного состава и его моральное разложение, нарушение нормальной работы тыла ВС;
- организация «управляемых кризисов», инициирование недовольства, беспорядков и панических настроений среди населения государства-противника.

Сочетается с мерами по укреплению морально-политического духа и патриотизма своих войск и населения страны.

ВОЙНА ИНФОРМАЦИОННО-ТЕХНИЧЕСКАЯ**,** широкомасштабное применение способов и средств информационного воздействия на технику и вооружение противника в интересах достижения поставленных целей. Война информационно техническая ведется как в мирное, так и в военное время с помощью информационно-технического оружия, включающего в себя в себя информационное оружие театра военных действий и программно-математическое оружие.

ВОЙНА СЕТЕВАЯ - принцип организации ведения военных действий, при котором силы и средства организуются не по принципу иерархического подчинения, а по принципу сети, соответственно меняется и принцип организации управления. Такой принцип традиционно используется крупными террористическими организациями. Применялся он и в партизанских движениях. Сетевой принцип используется хакерскими группами. Многие аналитики считают его основным в войне информационной.

ВРЕМЕННАЯ СТОЙКОСТЬ ЗАСЕКРЕЧИВАНИЯ ПЕРЕДАВАЕМЫХ СООБЩЕНИЙ - криптографическая стойкость засекречивания, при которой гарантируется скрытность содержания сообщения только в течение ограниченного, заранее обусловленного времени.

ВСПОМОГАТЕЛЬНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА И СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ - технические средства и системы, которые непосредственно не задействованы для обработки защищаемой информации, но находятся в электромагнитных полях побочных излучений технических средств обработки защищаемой информации, в результате чего на них наводится опасный сигнал, который по токопроводящим коммуникациям может распространяться за пределы контролируемой зоны.

ВТОРЖЕНИЕ - доступ неправомочный или проникновение любого рода (физическое или Информационное) в компьютеры, информационные системы и сети Непосредственно или опосредованно через корреспондирующие сети или системы. Синонимы: проникновение, доступ неправомочный.

ВТОРЖЕНИЕ ЭЛЕКТРОМАГНИТНОЕ - намеренное воздействие электромагнитной энергией на процессы обработки или передачи информации любым способом с целью их нарушения, изменения, в том числе изменения или нарушения обрабатываемой или передаваемой информации, обмана операторов или внесения беспорядка в организационные структуры обработки и передачи информации.

ВЫДЕЛЕННЫЕ СЕТИ СВЯЗИ - сети электросвязи физических и юридических лиц, не имеющие выхода на сеть связи общего пользования.

ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ - соединенная каналами связи система обработки данных, ориентированная на конкретного пользователя.

ГАММА ШИФРА - псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму для зашифрования открытых данных и их расшифрования.

ГАММИРОВАНИЕ - процесс наложения по определенному закону гаммы шифра на открытые данные.

ГАРАНТИРОВАННАЯ СТОЙКОСТЬ ЗАСЕКРЕЧИВАНИЯ ПЕРЕДАВАЕМЫХ СООБЩЕНИЙ - криптографическая стойкость засекречивания, при которой скрытность содержания сообщения,

безусловно, обеспечивается до момента полной потери оперативной ценности передаваемой информации.

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА – всемирная взаимосвязь сетей связи, компьютерной техники, баз данных и бытовой электроники, делающая доступной для пользователей обширные объемы информации.

ГОСУДАРСТВЕННАЯ БАЗА ДАННЫХ - база данных, созданная, приобретенная или накапливаемая за счет или с привлечением средств федерального бюджета.

ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ - политика, определяющая основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов РФ в этой области, порядок закрепления их обязанностей и ответственности за защищенность интересов РФ в информационной сфере в рамках закрепленных за ними направлений деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Основными направлениями государственной политики в сфере информатизации являются:

- обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы;
- формирование и защита государственных информационных ресурсов;
- создание и развитие федеральных и региональных информационных систем и сетей, обеспечение их совместимости и взаимодействия в едином информационном пространстве РФ;
- создание условий для качественного и эффективного информационного обеспечения граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений на основе государственных информационных ресурсов;
- обеспечение национальной безопасности в сфере информатизации, а также обеспечение реализации прав граждан, организаций в условиях информатизации;
- содействие формированию рынка информационных ресурсов, услуг, информационных систем, технологий, средств их обеспечения;
- формирование и осуществление единой технической и промышленной политики в сфере информатизации с учетом современного мирового уровня развития информационных технологий;
- поддержка проектов и программ информатизации;
- развитие законодательства в сфере информационных процессов, информатизации и ЗИ.

В международном сотрудничестве Российской Федерации основными направлениями обеспечения информационной безопасности являются:

- запрещение разработки, распространения и применения «информационного оружия»;
- обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;
- координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;
- предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми.

ГОСУДАРСТВЕННАЯ ТАЙНА - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ.

ГОСУДАРСТВЕННОЕ РЕГИОНАЛЬНОЕ СРЕДСТВО МАССОВОЙ ИНФОРМАЦИИ - средство массовой информации, учредителями которого выступают федеральные органы государственной власти совместно с органами государственной власти субъектов Российской Федерации либо

только органы государственной власти субъектов Российской Федерации.

ГОСУДАРСТВЕННОЕ ФЕДЕРАЛЬНОЕ СРЕДСТВО МАССОВОЙ ИНФОРМАЦИИ - средство массовой информации, учредителем которого выступает федеральный орган государственной власти.

ГОСУДАРСТВЕННЫЕ ОРГАНЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ - органы, предназначенные для непосредственного выполнения функций по обеспечению безопасности личности, общества и государства в системе исполнительной власти.

ГРИФ СЕКРЕТНОСТИ - реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и/или в сопроводительной документации на него. Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: особой важности, совершенно секретно и секретно.

ДАННЫЕ - 1) информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека; 2) представление фактов, суждений (знаний), или указаний формализованным способом в виде знаков или аналоговых сигналов, подходящим для связи, интерпретации или обработки автоматизированными средствами, а также восприятием человеком в любой доступной форме.

Сведения о лицах, предметах, событиях, явлениях и процессах независимо от формы их проявления, отображенные на материальном носителе, используемые в целях сохранения знаний.

ДЕЗИНФОРМАЦИЯ - 1) меры, направленные на введение в заблуждение противника с помощью подтасовки, искажения или фальсификации информации, вынуждающие его действовать в ущерб своим интересам; 2) заведомо ложные сведения, распространяемые или передаваемые с целью введения в заблуждение; 3) способ маскировки, заключающийся в преднамеренном распространении ложных сведений об объектах, их составе и деятельности, а также имитации их деятельности.

ДЕЗИНФОРМАЦИЯ ТЕХНИЧЕСКАЯ - создание ложной информации об объекте защиты путем воспроизведения несуществующих или искажения действительных демаскирующих признаков.

ДЕМОНСТРАЦИЯ - прием психологического воздействия в психологической операции, рассматриваемый как показ потенциальных возможностей субъекта воздействия к разрешению ситуации силовым путем с целью склонить объект (группу объектов) воздействия к капитуляции до применения реальных санкций.

ДЕШИФРОВАНИЕ - 1) процесс, обратный соответствующему обратимому процессу шифрования; 2) процесс, противоположный шифрованию. Широко используется для снятия шифров сигналов (сообщений) и распознавания результатов фотосъемки объектов разведки.

ДИВЕРСИЯ ИНФОРМАЦИОННАЯ - криминальное действие, по объективным признакам схожее с кибертерроризмом, однако в качестве цели имеющее подрыв экономической безопасности и обороноспособности.

ДИПОЛЬНЫЙ ОТРАЖАТЕЛЬ - средство пассивных помех, представляющее собой отрезок токопроводящего материала длиной, равной или кратной половине длине волны подавляемого радиоэлектронного средства.

ДОВЕДЕНИЕ СВЕДЕНИЙ - вид действия психологического. Доведение через СМИ или по другим каналам информации до субъекта, группы или общества с целью убедить объект воздействия (индивидуума или группу) изменить или сформировать мнения, эмоции, отношения и форму поведения, а в конечном итоге предпринять конкретные поступки в заданных интересах.

ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ -

совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения ИБ Российской Федерации.

ДОКУМЕНТ КОНФИДЕНЦИАЛЬНЫЙ - документ ограниченного доступа, на любом носителе, содержащий информацию, отражающую приоритетные достижения в сфере экономической, производственной, предпринимательской, управленческой и другой деятельности, а также информацию, состав которой является принадлежностью служебной деятельности. Утрата конфиденциального документа может нанести ущерб интересам или деловому *успеху собственника* или *владельца* информации. Под конфиденциальным (закрытым) документом понимается необходимым образом оформленный *носитель документированной информации*, содержащий сведения, которые относятся к *негосударственной тайне*, *составляют интеллектуальную собственность* юридического или физического лица и подлежат защите Называть конфиденциальные документы *секретными* или ставить на них гриф секретности не допускается Особенностью конфиденциального документа является то, что он представляет собой одновременно массовый носитель *ценной, защищаемой информации,* основной источник накопления и распространения этой информации, в том числе *неразглашения, утечки,* обязательный объект защиты.

ДОКУМЕНТ СЕКРЕТНЫЙ - документ на любом носителе, отнесенный к информационным ресурсам ограниченного доступа и содержащий сведения, составляющие государственную тайну, которые включены в утвержденный специальный перечень таких сведений.

ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ (ДОКУМЕНТ) - 1) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать; 2) зафиксированная на материальном носителе информация с указанием источника ее происхождения.

ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ С ОГРАНИЧЕННЫМ ДОСТУПОМ - по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную. Запрещено относить к информации с ограниченным доступом: законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации; документы, содержащие информацию о чрезвычайной ситуации, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом; документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением сведений, отнесенных к государственной тайне; документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений, организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

ДОМИНИРОВАНИЕ ИНФОРМАЦИОННОЕ - подавляющее преимущество, полученное через превышающую эффективность информационной деятельности (приобретение и использование данных, информации, знаний) в такой степени, что это преимущество демонстрируется практически через превышающую эффективность инструментальной деятельности.

ДОСТОВЕРНОСТЬ ИНФОРМАЦИИ - соответствие полученной информации действительной обстановке Достигается обозначением времени свершения событий, сведения о которых передаются; тщательным изучением и сопоставлением данных, полученных из различных источников; проверкой сомнительных сведений, своевременным скрытием дезинформационных и маскировочных мероприятий; исключением искаженной информации, передаваемой по техническим средствам.

ДОСТУП К ИНФОРМАЦИИ - 1) получение субъектом возможности ознакомления с информацией, в том числе с помощью технических средств; 2) ознакомление с информацией, ее

обработка, в частности, копирование, модификация или уничтожение.

ДОСТУП К ИНФОРМАЦИОННЫМ РЕСУРСАМ (СИСТЕМАМ) - совокупность средств массовой информации и механизмы доступа к открытым информационным ресурсам, устанавливаемые их собственниками.

ДОСТУП К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ - санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную или коммерческую тайну.

ДОСТУП К СВЕДЕНИЯМ, СОСТАВЛЯЮЩИМ ГОСУДАРСТВЕННУЮ ТАЙНУ - санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

ДОСТУП НЕПРАВОМОЧНЫЙ - доступ к ресурсу информационному, совершаемый в нарушение правил и полномочий (санкций), установленных для данного ресурса.

ДОСТУП ОГРАНИЧЕННЫЙ - доступ к ресурсу информационному, разрешаемый только определенному установленными для данного ресурса правилами и полномочиями (санкциями) кругу лиц.

ДОСТУП ТЕХНИЧЕСКИЙ - неправомочное изготовление (клонирование) телефонных трубок или платежных телефонных карт с фальшивыми идентификаторами абонентов, номеров и платежных отметок.

ДОСТУПНОСТЬ ИНФОРМАЦИИ - состояние информации, ее носителей и технологии обработки, при которых обеспечивается беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

ЖИВУЧЕСТЬ СИСТЕМЫ ВОЕННОЙ СВЯЗИ - способность системы военной связи обеспечивать управление войсками (силами) и оружием в условиях воздействия оружия противника.

ЖИЗНЕННО ВАЖНЫЕ ИНТЕРЕСЫ - совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

ЖУРНАЛИСТ - лицо, занимающееся редактированием, созданием, сбором или подготовкой сообщений и материалов для редакции зарегистрированного средства массовой информации, связанное с ней трудовыми или иными договорными отношениями либо занимающееся такой деятельностью по ее уполномочию.

ЗАКЛАДНОЕ УСТРОЙСТВО - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

ЗАКОН ИНФОРМАЦИОННОЙ БОРЬБЫ - существенное, необходимое, устойчиво повторяющееся отношение, характеризующее упорядоченность строения и функционирования, тенденции изменения и развития тех или иных явлений информационной борьбы.

ЗАКОНОМЕРНОСТЬ ИНФОРМАЦИОННОЙ БОРЬБЫ - подчиненность закону или указание на то, что в основе познания какого-либо явления ИБ лежит один или несколько законов. Понятие «закономерность» более предпочтительно в тех случаях, когда связи, повторяющиеся отношения ИБ недостаточно выражены количественно.

ЗАМЫСЕЛ ЗАЩИТЫ ИНФОРМАЦИИ - основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий,

необходимых для достижения цели ЗИ.

ЗАРАЖЕНИЕ - метод психологического воздействия в психологической операции, рассматриваемый как общественно-психологический процесс, выражающий бессознательную, невольную подверженность индивида (группы) эмоциональному воздействию других групп или большой массы людей в условиях непосредственного контакта.

ЗАСЕКРЕЧЕННАЯ СВЯЗЬ - связь, при которой информация, передаваемая по телефону, телеграфу, фототелеграфу, шифруется (дешифруется) аппаратурой засекречивания в процессе передачи (приема) Имеет целью скрыть информацию от ознакомления с ее содержанием.

ЗАШИФРОВАНИЕ ДАННЫХ - 1) процесс преобразования открытых данных в зашифрованные при помощи шифра; 2) процесс преобразования открытых данных в зашифрованные при помощи шифра.

ЗАШИФРОВАННЫЕ ДАННЫЕ - данные, хранящиеся в зашифрованном виде (в документах, в памяти ЭВМ и т.п.), те данные, к которым применен способ криптографической защиты.

ЗАЩИТА ВЫЧИСЛИТЕЛЬНОЙ СЕТИ - исключение несанкционированного доступа пользователей к элементам и ресурсам сети путем использования организационных мероприятий, аппаратных, программных и криптографических методов и средств.

ЗАЩИТА ДАННЫХ - 1) меры сохранения данных от нежелательных последствий, которые неумышленно или преднамеренно ведут к их модификации, раскрытию или разрушению; 2) процесс обеспечения сохранности, целостности и надежности обработки и хранения данных.

ЗАЩИТА ИНФОРМАЦИИ (ЗИ) - 1) деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию; 2) совокупность организационных, правовых, технических и технологических мер по предотвращению и отражению угроз ресурсам информационным и системам информационным, устранению их последствий.
Различают следующие виды ЗИ: защита информации от разведки, от утечки, от разглашения, от несанкционированного доступа, от негативного воздействия (непреднамеренного, несанкционированного).
ЗИ проводится для достижения следующих основных целей:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Защите подлежат следующие ресурсы:

- информация и данные (включая программное обеспечение и относящиеся к средствам защиты пассивные данные, такие как пароли);
- услуги передачи и обработки данных;
- оборудование и средства.

ЗАЩИТА ИНФОРМАЦИИ ОТ АГЕНТУРНОЙ РАЗВЕДКИ - деятельность, направленная на предотвращение получения защищаемой информации агентурной разведкой.

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕПРЕДНАМЕРЕННОГО ВОЗДЕЙСТВИЯ - 1) деятельность,

направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации; 2) деятельность по предотвращению воздействия на защищаемую информацию от ошибок пользователей информации, сбоев технических и программных средств информационных систем, а также природных явлений или иных нецеленаправленных воздействий, связанных с функционированием технических средств или с деятельностью обслуживающего персонала и пользователей, приводящих к искажению, уничтожению, копированию, блокированию информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ВОЗДЕЙСТВИЯ - деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА - деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

ЗАЩИТА ИНФОРМАЦИИ ОТ РАЗГЛАШЕНИЯ - деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации.

ЗАЩИТА ИНФОРМАЦИИ ОТ ТЕХНИЧЕСКОЙ РАЗВЕДКИ - деятельность, направленная на предотвращение получения защищаемой информации с помощью технических средств разведки.

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ - деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и добывания информации разведками.

ЗАЩИТА ОТ ИНФОРМАЦИОННОГО (ИНФОРМАЦИОННО-ТЕХНИЧЕСКОГО ВОЗДЕЙСТВИЯ) - действия по защитt информации, нейтрализации или снижению эффективности информационно-технического воздействия на информационно-технические системы и психику человека.

ЗАЩИТА ОТ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО (ПСИХОЛОГИЧЕСКОГО) ВОЗДЕЙСТВИЯ - комплекс мероприятий, направленных на защиту психики человека от несанкционированных информационно-психологических воздействий.

ЗАЩИТА ОТ НЕПРЕДНАМЕРЕННЫХ ВЗАИМНЫХ РАДИОЭЛЕКТРОННЫХ ПОМЕХ (ОБЕСПЕЧЕНИЕ ЭЛЕКТРОМАГНИТНОЙ СОВМЕСТИМОСТИ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ) - снижение (исключение) взаимного влияния излучения РЭС при их совместном применении в группировках своих войск (сил).

ЗАЩИТА ОТ СРЕДСТВ РАДИОЭЛЕКТРОННОГО ПОРАЖЕНИЯ ПРОТИВНИКА - организационно-технические мероприятия по обеспечению снижения эффективности воздействия на свои радиоэлектронные объекты средствами функционального поражения, радиоэлектронного подавления и самонаводящимся на источник радиоизлучение оружием. Защита от средств радиоэлектронного поражения противника включает защиту от средств функционального поражения, защиту от радиоэлектронного подавления и защиту от самонаводящегося на источник

электромагнитного оружия.

ЗАЩИТА ОТ СРЕДСТВ РАДИОЭЛЕКТРОННОЙ РАЗВЕДКИ ПРОТИВНИКА - исключение или существенное затруднение для противника добывания с помощью радиоэлектронных средств разведки сведений о радиоэлектронных системах (средствах) своих войск (сил) и объектов.

ЗАЩИТА ОТ СРЕДСТВ ФУНКЦИОНАЛЬНОГО ПОРАЖЕНИЯ - снижение эффективности воздействия на свои радиоэлектронные объекты средствами функционального поражения.

ЗАЩИТА ПРОГРАММНЫХ СРЕДСТВ - организационные, правовые, технические и технологические меры, направленные на предотвращение возможных несанкционированных действий по отношению к программным средствам и устранение последствий этих действий.

ЗАЩИЩАЕМАЯ ИНФОРМАЦИЯ - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или собственника информации. Собственником информации может быть: государство, юридическое лицо или физическое лицо, группа физических лиц.

ЗАЩИЩЕННОЕ СРЕДСТВО ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ (ЗАЩИЩЕННАЯ АВТОМАТИЗИРОВАННАЯ СИСТЕМА) - средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты.

ЗАЩИЩЕННОСТЬ ИНФОРМАЦИИ - соответствие эффективности защиты информации требованиям нормативных документов; способность системы противостоять несанкционированному доступу к конфиденциальной информации, ее искажению или разрушению. Защищенность информации можно рассматривать как с позиций технической защиты от несанкционированного доступа (свойство недоступности), так и социально-психологических по степени конфиденциальности и секретности (свойство конфиденциальности).

ЗАЩИЩЕННОСТЬ ОБЪЕКТА ЗАЩИТЫ - способность объекта защиты противостоять иностранным техническим разведкам и предотвращать утечку информации о нем по техническим каналам.

ЗАЩИЩЕННЫЕ СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ - средства вычислительной техники общего и специального назначения, защищенные от утечки, искажения или уничтожения информации за счет несанкционированного доступа.

ЗЛОУПОТРЕБЛЕНИЯ СВОБОДОЙ МАССОВОЙ ИНФОРМАЦИИ [при проведении агитации] — ...злоупотребления свободой массовой информации: агитация, возбуждающая социальную, расовую, национальную ненависть и вражду. призывы к захвату власти, насильственному изменению конституционного строя и нарушению целостности государства, пропаганда войны и иные формы злоупотребления свободой массовой информации, запрещенные федеральными законами.

ЗОМБИРОВАНИЕ – форсированная обработка подсознания человека, благодаря которой он теряет направляющий контакт со своим прошлым и программируется на безоговорочное, неосознаваемое подчинение приказам своего хозяина.

ИДЕНТИФИКАТОР ДОСТУПА - уникальный признак субъекта или объекта доступа.

ИДЕНТИФИКАЦИЯ - присвоение субъектам или объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

ИНДУКТИВНАЯ СВЯЗЬ - связь между электрическими цепями переменного тока за счет взаимодействия их магнитных полей в результате близкого параллельного расположения проводов. Является потенциальным каналом утечки информации при выходе проводов за пределы контролируемой территории.

ИНЖЕНЕРНО-ТЕХНИЧЕСКИЙ ЭЛЕМЕНТ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ - комплекс организационно-технических, технических и технологических мероприятий защиты информации, предназначенных для пассивного и активного *противодействия средствам* технической разведки и формирования рубежей *охраны территории, здания, помещений и оборудования* с помощью совокупности *технических средств.* Элемент включает: сооружения инженерной (физической) защиты от проникновения *посторонних лиц* на территорию, в здание и помещения фирмы; средства защиты *технических каналов* распространения и возможной *утечки информации;* средства защиты помещение от визуальных способов технической разведки; технические средства обеспечения охраны фирмы; средства противопожарной охраны; средства обнаружения приборов и устройств технической разведки; средства противодействия этим приборам и устройствам, технические средства контроля, предотвращающие вынос персоналом из помещений специально маркированных предметов, документов, дискет.

ИНТЕРЕСЫ В ИНФОРМАЦИОННОЙ СФЕРЕ - реальная причина действий, лежащая в основе мотивов развития информационной сферы государства, общества, личности. В Доктрине информационной безопасности РФ определены следующие интересы в сфере информационной безопасности государства, общества, личности.

ИНТЕРЕСЫ ГОСУДАРСТВА В ИНФОРМАЦИОННОЙ СФЕРЕ, состоят в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав человека и гражданина в области получения информации и пользования ею в целях незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, обеспечения законности и поддержания правопорядка, развития равноправного международного сотрудничества.

ИНТЕРЕСЫ ЛИЧНОСТИ В ИНФОРМАЦИОННОЙ СФЕРЕ, состоят в реализации конституционных прав и свобод на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также ЗИ, обеспечивающей личную безопасность.

ИНТЕРЕСЫ ОБЩЕСТВА В ИНФОРМАЦИОННОЙ СФЕРЕ, состоят в создании правового, социального государства, достижение и поддержание общественного согласия, духовного обновления России.

ИНФОРМАТИЗАЦИЯ - 1) организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти и местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов; 2) социально-экономический и научно-технологический процесс создания оптимальных условий удовлетворения информационных потребностей граждан, предприятий, организаций, государства, всех структур общества на основе организации информационных ресурсов с использованием перспективных информационных технологий.

ИНФОРМАЦИОННАЯ АГРЕССИЯ - монопольное владение значительной частью информационных ресурсов и доминирование с элементами диктата на рынке информационных услуг.

ИНФОРМАЦИОННАЯ АКЦИЯ - ограниченное по масштабу и времени информационное воздействие на конкретный информационный объект (группу объектов) противника и защита от аналогичных воздействий с его стороны.

ИНФОРМАЦИОННАЯ АТАКА - однократное информационное и/или физическое воздействие на одиночный информационный объект противника.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ИБ) - состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИЙСКОЙ ФЕДЕРАЦИИ - состояние

защищенности национальных интересов РФ в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ УПРАВЛЕНИЯ И СВЯЗИ ВС РФ - состояние информации и технических средств (систем) ее передачи и обработки, при котором обеспечивается использование информации и ТСПИ по их прямому назначению без ущерба для собственников и владельцев информации.

ИНФОРМАЦИОННАЯ ВОЙНА - широкомасштабная информационная борьба с применением способов и средств информационного воздействия на противника в интересах достижения целей воздействующей стороны.

По направленности информационных воздействий ИВ (борьба) подразделяется на два вида: *информационно-психологическую (психологическую) и информационно-техническую.* В *информационно-психологической борьбе* главными объектами воздействия и защиты являются психика личного состава Вооруженных Сил и населения противостоящих сторон, системы формирования общественного мнения и принятия решений, п*ри информационно-технической войне (борьбе)* - информационно-технические системы (системы связи и управления, телекоммуникационные системы, радиоэлектронные средства, компьютерные сети и т.д.).

ИВ может проводиться во всех сферах общественной жизни – в экономике, политике, в военном деле, в социальных отношениях, в сфере духовной жизни и особенно в идеологии.

Как и любая война ИВ предполагает наступательную и оборонительную сторону.

ИВ осуществляется при помощи информационного оружия.

ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА - 1) технические средства и системы формирования, обработки, хранения и передачи информации. Является средой, которая обеспечивает возможность сбора, передачи, хранения, автоматизированной обработки и распространения информации в обществе; 2) среда, которая обеспечивает возможность сбора, передачи, хранения, автоматизированной обработки и распространения информации в обществе. Образуется совокупностью информационно-телекоммуникационных систем и сетей связи, индустрии средств информатизации, телекоммуникации и связи; системы формирования и обеспечения сохранности информационных ресурсов; системы обеспечения доступа к информационно-телекоммуникационным системам, сетям связи и информационным ресурсам; индустрии информационных услуг и информационного рынка; системы подготовки и переподготовки кадров, проведения научных исследований; 3) совокупность центров обработки и анализа информации, каналов информационного обмена и телекоммуникации, линий связи, систем и средств защиты информации.

ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА СИСТЕМЫ (СЕТИ) СВЯЗИ - совокупность информационных подсистем, центров управления, аппаратно-программных средств и технологий обеспечения сбора, хранения, обработки и передачи информации в системе (сети) связи.

ИНФОРМАЦИОННАЯ КАМПАНИЯ – форма информационного противоборства, образуемая совокупностью ряда операций, других видов деятельности органов власти Российской Федерации, согласованных по целям и задачам, проводимых по единому замыслу на нескольких направлениях (в нескольких регионах).

ИНФОРМАЦИОННАЯ МОДЕЛЬ - количественно-качественное описание возможного варианта построения системы информационной, предусматривающее определение ее целей и задач, структуры, связей, оценку возможных угроз и механизмов повышения защищенности системы от этих угроз.

ИНФОРМАЦИОННАЯ ОБСТАНОВКА – совокупность факторов и условий, в которых осуществляется борьба Российской Федерации в информационной сфере в целях реализации своих национальных интересов.

Основные элементы информационной обстановки:

- факты ведения информационного противоборства в отношении Российской Федерации;
- концепции, замыслы и планы использования информационной сферы иностранными

государствами (другими силами), затрагивающие национальные интересы Российской Федерации;
- позиции и личные качества политических и военных лидеров иностранных государств (других сил), а также международных (неправительственных) организаций;
- потенциал систем формирования общественного мнения иностранных государств (других сил), а также международных (неправительственных) организаций;
- состав и возможности сил и средств информационного противоборства иностранных государств (других сил);
- состояние защищенности их критически важных информационных объектов;
- состав и возможности системы информационного противоборства Российской Федерации;
- состояние защищенности ее критически важных объектов информационной инфраструктуры;
- временные, пространственные, правовые, материально-технические и другие ограничения для применения сил и средств информационного противоборства в отношении иностранных государств (других сил) и иные.

ИНФОРМАЦИОННАЯ СИСТЕМА - 1) полная инфраструктура, организация, персонал и компоненты, которые участвуют в сборе, обработке (изменении, обновлении), хранении, передаче, демонстрации и распространении информации; 2)организационно упорядоченная совокупность документов и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы; 3) организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи; 4) организационно упорядоченная совокупность специалистов, информационных ресурсов, технологий, осуществляющая информационные процессы.

ИНФОРМАЦИОННАЯ СФЕРА (СРЕДА) - 1) сфера (среда) деятельности субъектов, связанная с созданием, преобразованием и потреблением информации; 2) совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ - 1) согласованная совокупность информационных способов и средств, предназначенная для создания, хранения, обработки, передачи и использования информации; 2) приемы, способы и методы применения средств вычислительной техники при выполнении функций хранения, обработки, передачи и использования данных.

ИНФОРМАЦИОННОЕ АГЕНТСТВО - организация, осуществляющая сбор и оперативное распространение информации.

ИНФОРМАЦИОННОЕ ВОЗДЕЙСТВИЕ - 1) акт применения оружия информационного, а также непосредственное воздействие на элементы пространства информационного противника иными методами с целью нанесения ущерба; 2) согласованные по целям, задачам, месту и времени мероприятия по воздействию информационных и программных средств на информацию и на информационные объекты противника.

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ - совокупность форм документов, классификаторов, нормативной базы и реализованных решений по объемам, размещению и формам существования информации, применяемой в автоматизированной системе при ее функционировании.

ИНФОРМАЦИОННОЕ ОБЩЕСТВО - состояние развития общественных и прежде всего производственных отношений, при котором основная часть валового продукта производится не за счет материального производства, а на основе создания и продажи наукоемких технологий, информационных продуктов, т.е. результатов интеллектуального труда граждан.

ИНФОРМАЦИОННОЕ ОРУЖИЕ - совокупность способов и средств информационного воздействия на технику и людей с целью решения задач воздействующей стороны. В соответствии

с видами информационной борьбы ИОр подразделяется на два основных вида: информационно-техническое и информационно-психологическое. Главными объектами информационного оружия первого вида является *техника*, второго – *люди*.

ИНФОРМАЦИОННОЕ ОРУЖИЕ ТЕАТРА ВОЕННЫХ ДЕЙСТВИЙ (ИОР ТВД) - совокупность средств управления, связи, разведки, навигации и РЭБ чаще всего в сочетании с высокоточным оружием, применяемое для достижения информационного превосходства на поле боя.

Стратегическое информационное оружие ТВД - совокупность информационных способов и средств, способных нанести неприемлемый ущерб политическим, экономическим и военным интересам страны, а также другим структурам, образующим ее стратегический потенциал, в рамках стратегической операции вооруженных сил государства.

Оперативное информационное оружие ТВД - совокупность информационных способов и средств, способных обеспечить решение важных задач при проведении операции вооруженных сил на определенном театре военных действий.

Тактическое информационное оружие ТВД - совокупность информационных способов и средств, способных обеспечить решение важных задач в ходе боевых действия или боя.

ИНФОРМАЦИОННОЕ ПРЕВОСХОДСТВО - степень доминирования в информационной области, которая разрешает проведение действий без опасности эффективного противодействия. В военной трактовке: возможность сбора, обработки и распространения непрерывного потока информации, в то же время используя в своих целях или не давая возможности противнику делать то же самое.

ИНФОРМАЦИОННОЕ ПРОГРАММНО-МАТЕМАТИЧЕСКОЕ ОРУЖИЕ (ИПМОр) - совокупность способов и средств, позволяющая целенаправленно изменять (уничтожать, искажать), копировать, блокировать информацию, преодолевать системы защиты, ограничивать допуск законных пользователей, осуществлять дезинформацию, нарушать функционирование носителей информации, дезорганизовывать работу технических средств, компьютерных систем и информационно-вычислительных сетей, применяемая в ходе информационной борьбы (войны) для достижения поставленных целей.
ИПМОр подразделяется на два типа:

- способы и средства воздействия на программный ресурс электронных управляющих модулей;
- способы и средства воздействия на процесс передачи информации.

ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО - 1) форма межгосударственного противоборства, предусматривающая целенаправленное использование специально разработанных средств для воздействия на ресурс информационный противостоящей стороны и защиты собственных ресурсов в интересах достижения поставленных политических и военных целей; 2) форма межгосударственного соперничества, реализуемая посредством оказания воздействия информационного на системы управления других государств и их вооруженных сил, а также на политическое и военное руководство и общество в целом, инфраструктуру информационную и СМИ этих государств для достижения выгодных себе целей при одновременной защите от аналогичных действий своего пространства информационного.

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ СФЕРА - часть информационной сферы, связанная с воздействием информации на психическую деятельность человека. Она образуется совокупностью людей, информацией, которой они обмениваются и которую воспринимают, общественных отношений, возникающих в связи с информационным обменом, и информационными воздействиями на психику человека.

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЕ (ПСИХОЛОГИЧЕСКОЕ) ОРУЖИЕ - совокупность способов и средств (технологий) открытого (или полускрытого) воздействия на психику людей, применяемая в ходе информационно-психологической борьбы (войны) для достижения поставленных целей.

"Чистые"(честные) информационно-психологические технологии включают в себя такие приемы как открытая дискуссия, спор, беседа, коллоквиум и т.д., в процессе которых одна сторона убеждает (побеждает) своего оппонента логикой мысли, обращением к разуму, приведением

убедительных доводов.

Появление “грязных” (манипулятивных) технологий увязывается с глобализацией средств массовой информации (СМИ), оказывающих существенное влияние на формирование у людей различных точек зрения на различные политические и социальные процессы и явления, на события международного и внутригосударственного планов, на формирование их отношений к политическим и партийным лидерам, первым лицам государства. В наборе “грязных” технологий состоят: дезинформация, ложь, подтасовка фактов, извращение содержания сообщений, действий, поступков, подчеркивание отрицательных и замалчивание положительных сторон проблемы (личности), чередование правдивой информации с ложной и т.д. и т.п. “Грязные” технологии реализуются, как правило, через все виды СМИ в течение длительного времени. Внедрение агентуры влияния в СМИ противоборствующего государства позволяет манипулировать общественным сознанием народа, применять специальные средства его зомбирования - информационно-психологические технологии скрытого (тайного) воздействия, которые составляют физическую сущность *психофизического оружия*.

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЕ ВОЗДЕЙСТВИЕ (в псих. борьбе) - 1) один из видов психологического воздействия на индивидуальное и общественное сознание объекта (групп объектов) воздействия с преимущественным использованием информации, подготовленной соответствующим образом и доводимой до объекта (групп объектов) воздействия с помощью различных форм психологического воздействия (печатными средствами, с помощью радио- и телевещания, изобразительными средствами, через непосредственное общение, материальными акциями, через информационные компьютерные сети); 2) комплекс специальных действий (психологических операций, мероприятий и акций), проводимых в рамках психологического воздействия, осуществляемых с помощью информации(пропаганды и агитации), подготовленной соответствующим образом и доводимой до объекта (групп объектов) воздействия с помощью различных форм психологического воздействия (печатными средствами, с помощью радио- и телевещания, изобразительными средствами, через непосредственное общение, материальными акциями, через информационные компьютерные сети).

ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМА - совокупность информационно-вычислительных систем, объединенных системой передачи данных. Информационно-вычислительные системы реализуют функции автоматизации процессов сбора, обработки и хранения информации, а системы передачи данных позволяют осуществлять обмен этой информацией между информационно-вычислительными системами, а также обеспечивать доступ удаленных пользователей к хранящейся и обрабатываемой информации.

ИНФОРМАЦИОННО-ТЕХНИЧЕСКОЕ ВОЗДЕЙСТВИЕ - применение способов и средств информационного воздействия на информационно-технические объекты страны, на технику и вооружение противника в интересах достижения поставленных целей.

ИНФОРМАЦИОННЫЕ ОТНОШЕНИЯ - общественные отношения, складывающиеся в процессе сбора, обработки, хранения, передачи и распространения информации.

ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ - 1) процессы сбора, обработки, накопления, хранения, поиска и распространения информации; 2) процессы создания, сбора, обработки, накопления, хранения, поиска, распространения и потребления информации; 3) процессы создания, обработки, хранения, защиты от внутренних и внешних угроз, передачи, получения, использования и уничтожения информации; 4) процессы сбора, обработки, накопления, хранения, актуализации, распространения информации.

ИНФОРМАЦИОННЫЕ РЕСУРСЫ - 1) инфраструктура информационная, а также информационные массивы, базы данных и собственно информация и ее потоки; 2) отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах); 3) отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других видах информационных систем); 4) документы и массивы документов

(библиотеки, архивы, фонды, базы данных, базы знаний), другие формы организации информации по всем направлениям жизнедеятельности общества.

ИНФОРМАЦИОННЫЙ ОБЪЕКТ - элемент программы, содержащий фрагменты информации, циркулирующей в программе. В зависимости от языка программирования в качестве информационных объектов могут выступать переменные, массивы, записи, таблицы, файлы, фрагменты оперативной памяти и т. п..

ИНФОРМАЦИОННЫЙ ТЕРРОРИЗМ - 1) использование информационных средств в террористических целях, угрозы применения или применения физического насилия в политических целях, запугивания и дестабилизации общества, и таким образом оказания влияния на население или государство; 2) действия по дезорганизации автоматизированных информационных систем, создающие опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, если они совершены в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти, а также угроза совершения указанных действий в тех же целях. В узко правовом смысле информационный терроризм может трактоваться как намеренное злоупотребление средствами информационной системы, информационной сети или их компонентом в целях поддержания или способствования террористической деятельности или отдельному такому действию. В этом случае злоупотребление системой (сетью) не обязательно приводит к прямому насилию против людей, но может быть причиной катастроф или диверсий, в результате которых могут быть человеческие жертвы.

ИНФОРМАЦИЯ - 1) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления; 2) свойство материи выступать в виде некоторого разнообразия (объектов, элементов, характеристик) и отражать это разнообразие, проявляющееся, в частности, в сведениях, извлекаемых людьми (машинами) в результате соответствующей обработки наблюдений окружающего мира, анализируемых ими и используемых в целях коммуникации (связи) и управления.

ИНФОРМАЦИЯ АУТЕНТИФИКАЦИИ - информация, используемая для установления подлинности запрашиваемой личности.

ИНФОРМАЦИЯ КОНФИДЕНЦИАЛЬНАЯ - 1) сведения, не отнесенные к государственной тайне, доступ к которым ограничивается в соответствии с законодательством РФ. К ней относятся сведения, составляющие служебную и коммерческую тайны, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, личную и семейную тайну, а также сведения, раскрывающие частную жизнь граждан; 2) служебная, профессиональная, промышленная, коммерческая или иная информация, правовой режим которой устанавливается ее собственником на основе законов о коммерческой, профессиональной (промышленной) тайне, государственной *службе и* других законодательных актов.

ИНФОРМАЦИЯ ОГРАНИЧЕННОГО ДОСТУПА - 1) вид сведений, доступ к которым ограничен в соответствии с законодательством и разглашение которых может нанести ущерб интересам других лиц, общества и государства. В составе такой информации различают сведения, составляющие государственную тайну, и информацию конфиденциальную; 2) сведения, доступ к которым ограничен в соответствии с законодательством и разглашение которых может нанести ущерб интересам других лиц, общества и государства. В составе такой информации различают сведения, составляющие государственную тайну, и конфиденциальную информацию; 3) подразделяется на секретную и конфиденциальную.

ИНФОРМАЦИЯ, ПОДЛЕЖАЩАЯ ЗАЩИТЕ - любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу.

ИНФОРМИРОВАНИЕ - 1) донесение до сознания человека (группы людей) новой информации; 2) (в психол. безоп.), прием психологического воздействия психологической операции,

рассматриваемый как донесение до сознания объекта (группы объектов) новых сведений о лицах, предметах, фактах, событиях, явлениях и процессах, знаний в виде таких значений общественного опыта, которые не несут личностного смысла и не затрагивают главных потребностей, интересов, ценностных ориентации, установок личности, но способных создавать, пополнять, изменять, дезавуировать представления людей.

ИНФРАСТРУКТУРА ЗАЩИТЫ ИНФОРМАЦИИ - разделенная или связанная совокупность компьютеров, коммуникаций, данных, технологий и систем безопасности, систем обучения, обеспечения, использования и подготовки кадров и других структур поддержки всех форм безопасности информации и информационных инфраструктур всех уровней для данного объекта, структуры, территории.

ИНФРАСТРУКТУРА ИНФОРМАЦИОННАЯ - технические средства и системы формирования, обработки, хранения и передачи информации. Является средой, которая обеспечивает возможность сбора, передачи, хранения, автоматизированной обработки и распространения информации в обществе.

ИНЦИДЕНТ - проанализированный случай попытки получения доступа несанкционированного или нападения информационного на автоматизированную информационную систему. Он включает несанкционированное зондирование и просматривание; прерывание или воспрещение обслуживания; искаженный или уничтоженный ввод, обработку, хранение или вывод информации; или внесение изменений в характеристики аппаратного оборудования, программно-аппаратных средств или программного обеспечения информационной системы с (или без) ведома, инструкции или намерения пользователя.

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИИ НЕПРАВОМЕРНОЕ - передача, распространение (публикация), применение в действиях информационных полученных легальным путем сведений в нарушение правил и полномочий (санкций), установленных для данных сведений и субъекта, предпринявшего такие действия.

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И ИНФОРМАЦИОННЫХ РЕСУРСОВ НЕПРАВОМЕРНОЕ - использование телекоммуникационных и информационных систем и ресурсов без соответствующих прав или с нарушением установленных правил, законодательства или норм международного права.

ИСТОЧНИК УГРОЗЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ - объективные и субъективные явления, события, факторы, действия и обстоятельства, содержащие опасность для ценной информации. К объективным источникам можно отнести: *экстремальные ситуации*, несовершенство технических средств и др. Субъективные источники связаны с человеческим фактором и включают: *злоумышленников* различного рода, *посторонних лиц*, посетителей, неквалифицированный или безответственный персонал, психически неполноценных людей, сотрудников, обиженных руководством фирмы, и др. Источники угрозы могут быть внешними и внутренними. Внешние источники находятся вне фирмы и представлены чрезвычайными событиями, а также организационными структурами и физическими лицами, проявляющими определенный интерес к фирме. Внутренние источники угрозы связаны с фатальными событиями в здании фирмы, а также с персоналом. Однако наличие источника угрозы не является *угрозой*. Угроза реализуется в действиях.

ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ - внешние и внутренние.

Внешние источники:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Внутренние источники:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

ИФОРМАЦИОННАЯ ЗАЩИТА - совокупность информационных средств, обеспечивающих (предназначенных для) противодействие воздействию информационному, включая атаки информационные, а также реализуемым на каналах распространения информации (СМИ, сети передачи данных и т.п.) действиям психологическим.

КАМУФЛЯЖ - способ маскировки, при котором на маскируемый предмет наносятся пятна, полосы различных цветов и размеров, затрудняющие их опознавание визуально-оптическими и фотографическими средствами разведки.

КАНАЛ ПРОНИКНОВЕНИЯ - физический путь от злоумышленника к источнику конфиденциальной информации, посредством которого возможен несанкционированный доступ к охраняемым сведениям.

КАНАЛ СВЯЗИ - физическая среда, аппаратные и в некоторых каналах программные средства передачи информации.

КАНАЛ УТЕЧКИ ИНФОРМАЦИИ - физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможно несанкционированное получение охраняемых сведений (совокупность источника коммерческой тайны, физической среды и средства промышленного шпионажа).

КАНАЛ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ - совокупность источника речевой информации, среды распространения акустических сигналов и акустического приемника, обуславливающая возможность перехвата речевой информации.

КАТЕГОРИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ - уровень безопасности информации, определяемый установленными нормами в зависимости от важности (ценности) информации.

КАЧЕСТВО СЛУЖБЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ СВЯЗИ - совокупность определяемых, измеряемых и регулируемых параметров предотвращения, обнаружения и устранения угрозы ИБ сети связи.

КЛАССИФИКАЦИЯ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ - деление методов защиты информации по направлениям на основе общности однородных признаков.

КЛАССЫ МЕХАНИЗМОВ ЗАЩИТЫ - все механизмы защиты относятся к одному из перекрывающихся классов: предотвращение, обнаружение, восстановление.

КЛЮЧ КРИПТОГРАФИЧЕСКИЙ - последовательность символов, которые управляют процедурами шифрования и дешифрования.

КОД - система условных обозначений (группа цифр, букв или других символов) для скрытия передачи сведений конфиденциального характера по техническим средствам связи.

КОДИРОВАНИЕ - преобразование с помощью кодов открытого текста в условный с целью скрыть от злоумышленника содержание передаваемой по каналам связи информации.

КОММУНИКАЦИОННЫЙ КАНАЛ - элемент структуры психологического воздействия, рассматриваемый как канал, посредством которого осуществляется психологическое воздействие. Одно и то же сообщение может быть передано с помощью различных коммуникационных каналов: средств массовой информации, межличностного общения и т.д.

КОМПЛЕКС РАДИОЭЛЕКТРОННОГО ПОДАВЛЕНИЯ - совокупность средств РЭП, непосредственной (исполнительной) радиоэлектронной разведки и управления ими, других обеспечивающих средств и устройств, конструктивно и функционально связанных и совместно используемых для радиоэлектронного подавления.

КОМПЛЕКС СРЕДСТВ ЗАЩИТЫ - 1) совокупность всех (программно-технических) средств защиты; 2) совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения защиты объекта, автоматизированных систем и средств вычислительной техники.

КОМПЛЕКС ТЕХНИЧЕСКОГО КОНТРОЛЯ - совокупность средств измерения, регистрации, обработки результатов контроля и средств управления ими, конструктивно и функционально связанных и совместно используемых для комплексного технического контроля.

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ - реализация требований по защите от несанкционированного доступа к информации, от утечки по техническим каналам, от возможно внедренных специальных электронных устройств и программ - «вирусов».

КОМПЛЕКСНЫЙ ТЕХНИЧЕСКИЙ КОНТРОЛЬ - выявление достаточности и эффективности

мероприятий по противодействию техническим средствам разведки иностранных государств (противника), а также проверки выполнения установленных норм и требований по радиоэлектронной защите своих радиоэлектронных систем и средств. Различают радио, фотографический, визуально-оптический, телевизионный, радиолокационный, инфракрасный, химический, акустический, гидроакустический, радиотепловой контроль, контроль лазерных излучений и контроль эффективности защиты информации от ее утечки при эксплуатации технических средств передачи и обработки информации.

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ - защита АИС с использованием мер и "средств (организационных и программно-технических), которые гарантируют конфиденциальность, целостность и пригодность информации, хранимой и обрабатываемой с использованием компьютерных средств; они включают технологию, процедуры, и аппаратные средства ЭВМ и компоненты программного обеспечения, необходимые для защиты систем вычислительных комплексов и информации, обрабатываемой, хранимой и передаваемой как внутри системы так и от нее к другим информационно-вычислительным системам.

КОНСТИТУЦИОННЫЕ ПРАВА И СВОБОДЫ ЧЕЛОВЕКА И ГРАЖДАНИНА (В ИНФОРМАЦИОННОЙ СФЕРЕ) - права и свободы человека и гражданина, гарантируемые Конституцией Российской Федерации в информационной сфере к основным из них отнесены:

- право на личную и семейную тайну (ст. 23);
- право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23);
- право ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы (ст. 24);
- право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст. 29);
- свобода массовой информации (ст. 29);
- право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей (ст. 41);
- право на благоприятную окружающую среду, достоверную информацию о ее состоянии (ст. 42).

КОНТРДЕЗИНФОРМАЦИЯ - усилия по воспрещению, нейтрализации, уменьшению последствий или по извлечению выгод из операций противника по дезинформации.

КОНТРОЛИРУЕМЫЙ ПАКЕТ - прием атаки, при котором нападавшие тайно вставляют программу в отдаленных переключателях или хостах сети. Программа контролирует информационные пачки, посланные через сети, и посылает копию восстановленной информации хакеру. Анализируя полученные таким образом первые 125 символов связи, нападавшие могут изучать пароли и идентификаторы пользователя, которые, в свою очередь, они могут использовать, чтобы проникнуть в системы.

КОНТРОЛЬ ДОСТУПА - предупреждение несанкционированного доступа к защищенным данным.

КОНТРОЛЬ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ - проверка соответствия организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов в области ЗИ.

КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ - проверка соответствия организации и эффективности ЗИ установленным требованиям и/или нормам защиты.

КОНТРОЛЬ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ - 1) проверка соответствия качественных и количественных показателей эффективности мероприятий по ЗИ требованиям или нормам эффективности ЗИ; 2) проверка соответствия эффективности мероприятий по ЗИ установленным требованиям или нормам эффективности защиты.

КОНТРРАЗВЕДЫВАТЕЛЬНАЯ ДЕЯТЕЛЬНОСТЬ - деятельность органов ФСБ в пределах своих

полномочий по выявлению, предупреждению, пресечению разведывательной и иной деятельности специальных служб и организаций иностранных государств, а также отдельных лиц, направленной на нанесение ущерба безопасности России. Основаниями для осуществления органами ФСБ контрразведывательной деятельности является необходимость обеспечения защиты сведений, составляющих государственную тайну. Осуществление контрразведывательной деятельности, затрагивающей тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений граждан, допускается только на основании судебного решения.

КОНФИДЕНЦИАЛЬНОСТЬ - свойство, позволяющее не давать права на доступ к информации или не раскрывать ее неполномочным лицам, логическим объектам или процессам.

КОНЦЕПЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ - система взглядов, требований и условий организации защиты охраняемых сведений от разглашения, утечки и несанкционированного доступа к ним через различные каналы.

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - совокупность официальных взглядов на обеспечение безопасности информационной, методы и средства защиты жизненно важных интересов личности, общества и государства в информационной сфере.

КОНЦЕПЦИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ - система взглядов на обеспечение в РФ безопасности личности, общества и государства от внешних и внутренних угроз во всех сферах жизнедеятельности.

КРИПТОАНАЛИЗ - 1) раскрытие зашифрованного криптографическими методами текста с помощью известного ключа или без него (за счет вскрытия неизвестного ключа); 2) анализ криптографической системы и/или чувствительности данных, включая открытый текст; 3) анализ криптографической системы и ее входных и выходных данных с целью определения засекреченных переменных и значимой информации, включая открытый текст.

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА - защита данных при помощи криптографического преобразования данных.

КРИПТОГРАФИЧЕСКОЕ ПРЕОБРАЗОВАНИЕ - преобразование данных при помощи шифрования и (или) выработки имитосвязи.

КРИПТОГРАФИЯ - 1) наука об использовании математических методов и технических средств для преобразования открытой защищаемой информации в закрытую, зашифрованную форму, затрудняющую восстановления открытой информации; 2) тайнопись, система изменения информации (текста, речи) с целью сделать ее непонятной для непосвященных лиц; 3) дисциплина, охватывающая принципы, средства и методы преобразования данных для сокрытия их информационного содержимого, предотвращения их не обнаруживаемой модификации и/или их несанкционированного использования.

КРИПТОЛОГИЯ - наука о безопасности (секретности) передачи информации; включает криптографию (шифрование) и криптоанализ.

КРИТИЧЕСКАЯ ИНФОРМАЦИЯ - определенные факты относительно намерений, способностей и действий, жизненно необходимых для эффективного управления и деятельности структур критически важных, эффективного выполнения стоящих стратегических задач.

КРИТИЧЕСКАЯ ТЕХНОЛОГИЯ – протекающий во времени процесс обработки информационных и (или) материальных ресурсов, выход из которого за допустимые пределы может привести к нанесению ущерба национальным интересам России.

КРИТИЧЕСКИ ВАЖНЫЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ – информационно-телекоммуникационные системы, выход из строя или нарушение режима функционирования которых может оказать негативное влияние на состояние национальной

безопасности Российской Федерации.

КРИТИЧЕСКИ ВАЖНЫЕ ИНФОРМАЦИОННЫЕ ОБЪЕКТЫ, информационные объекты, воздействуя на которые возможно нанести максимальный ущерб (прекратить функционирование) информационной инфраструктуре государства (вооруженных сил) стратегического или оперативного уровня и привести к существенным отрицательным последствиям в политической, экономической, международной, оборонной, информационной и внутриполитической сферах деятельности государства.

КРИТИЧЕСКИ ВАЖНЫЕ СТРУКТУРЫ - 1) элементы политико-экономической структуры государства, дестабилизация или блокирование деятельности которых катастрофически скажется на функционировании государства в целом; 2) объекты, системы и институты государства, целенаправленное воздействие на ресурсы информационные которых может иметь последствия, прямо затрагивающие национальную безопасность (транспорт, энергоснабжение, кредитно-финансовая сфера, связь, органы государственного управления, система обороны, правоохранительные органы, стратегические информационные ресурсы, научные объекты и научно-технические разработки, объекты повышенной технической и экологической опасности, органы ликвидации последствий стихийных бедствий и иных чрезвычайных ситуаций).

КРИТИЧЕСКИ ВАЖНЫЙ СЕГМЕНТ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ – такая информационно-телекоммуникационная система (ИТС), выход из строя или нарушение режима функционирования которой может оказать негативное влияние на состояние национальной безопасности Российской Федерации.

К критически важным сегментам можно отнести:

- системы телекоммуникаций военного и специального назначения;
- системы управлений энергетикой, транспортом, водными системами;
- ИТС служб реагирования на чрезвычайные ситуации;
- банковские и финансовые ИТС;
- другие государственные и частные ИТС, минимально необходимые для функционирования экономики и государства.

ЛОЖНАЯ РАДИОЛОКАЦИОННАЯ ЦЕЛЬ - ложная цель, имитирующая реальные объекты (цели) для радиолокационной разведки.

ЛОЖНАЯ ЦЕЛЬ - техническое устройство, средство радиоэлектронного подавления или образование в среде распространения электромагнитных, акустических излучений, предназначенные для имитации реальных объектов для РЭС разведки и управления оружием путем излучения, ретрансляции или отражения сигналов, энергетические и спектральные характеристики которых близки к аналогичным характеристикам сигналов, излучаемых или отражаемых реальными объектами.

ЛОЖНЫЕ ИНФОРМАЦИОННЫЕ ОБЪЕКТЫ - объекты, имитирующие реальные ИО или преднамеренная выдача второстепенных ИО за критически важные для вызова по ним атак противника и отвлечения его сил и средств.

МАКРОВИРУСЫ - программы на языках (макроязыках), встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

МАНИПУЛЯЦИЯ - вид психологического воздействия, искусное исполнение которого ведет к скрытому возбуждению у другого человека намерений, не совпадающих с его актуально существующими желаниями.

Наряду с основным определением часто употребляются упрощенные формулировки определения межличностной манипуляции:

Манипуляция — это вид психологического воздействия, при котором мастерство манипулятора используется для скрытого внедрения в психику адресата целей, желаний,

намерений, отношений или установок, не совпадающих с теми, которые имеются у адресата в данный момент.

Манипуляция — это психологическое воздействие, нацеленное на изменение направления активности другого человека, выполненное настолько искусно, что остается незамеченным им.

Манипуляция — это психологическое воздействие, направленное на неявное побуждение другого к совершению определенных манипулятором действий.

Манипуляция — это искусное побуждение другого к достижению (преследованию) косвенно вложенной манипулятором цели.

Манипуляция — это действия, направленные на «прибирание к рукам» другого человека, помыкание им, производимые настолько искусно, что у того создается впечатление, будто он самостоятельно управляет своим поведением.

МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СЗИ – совокупность математических методов, моделей и алгоритмов для решения задач оценки опасности и мер защиты информации.

МАТЕРИАЛЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ – основное средство доведения информации, подготовленной соответствующим образом, до объектов (групп объектов) воздействия.

МАТЕРИАЛЬНО-ВЕЩЕСТВЕННЫЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ – это физический путь от источника (носителя) к злоумышленнику в виде жестких масс, жидкостей или газообразных веществ.

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ ПРЕСТУПНОСТЬ – использование телекоммуникационных и информационных систем и ресурсов и воздействие на такие системы и ресурсы в международном информационном пространстве в противоправных целях.

МЕЖДУНАРОДНЫЙ ИНФОРМАЦИОННЫЙ ОБМЕН – передача и получение информационных продуктов, а также оказание информационных услуг через Государственную границу.

МЕРОПРИЯТИЕ ПО ЗАЩИТЕ ИНФОРМАЦИИ – совокупность действий, направленных на разработку и/или практическое применение способов и средств ЗИ. Подразделяются на организационные, технические, программные.

МЕРОПРИЯТИЕ ПО КОНТРОЛЮ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ – совокупность действий, направленных на разработку и(или) практическое применение способов и средств контроля эффективности ЗИ.

МЕТКА КОНФИДЕНЦИАЛЬНОСТИ – элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте.

МЕТОД (СПОСОБ) КОНТРОЛЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ – порядок и правила применения определенных принципов и средств контроля эффективности ЗИ.

МЕТОД АНАЛИЗА ИНФОРМАЦИИ – совокупность правил, приемов, операций по выделению, отбору, систематизации, преобразованию, переработке и обобщению различных сведений, фактов и данных, получаемых от конкретного источника. Позволяет выделить наиболее существенную информацию, наметить пути получения новой информации, которая явно не содержится в имеющихся данных, прийти от единичных фактов к общим закономерностям. Известны сравнение, абстрагирование, аналогия, обобщение информации.

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ – выборочно применяемые универсальные и специфические способы (приемы, меры, мероприятия) реализации элементов в *системы защиты информации* и входящих в них содержательных частей для формирования комплексной и индивидуальной структуры данном системы. К универсальным способам можно отнести регламентацию процесса, выделение процесса, скрытие процесса или информации, ограничение доступа к процессу или информации, дезинформацию конкурента *или злоумышленника*, *расчленение (дробление)*

информации, *тайны*, создание физических и иных препятствий на пути злоумышленника (рубежей защиты) Специфические способы обеспечивают индивидуализацию системы в зависимости от поставленных задач *защиты информации* в конкретной фирме.

МЕХАНИЗМЫ ЗАЩИТЫ – последовательность проведения мероприятий и процессов по предотвращению утечки информации и ЗИ.
ВИДЫ МЕХАНИЗМОВ ЗАЩИТЫ: методы криптографирования и шифрование, аспекты административного управления ключами, механизмы цифровой подписи, механизмы управления доступом, механизмы целостности данных, механизмы обмена информацией аутентификации, механизмы заполнения трафика, механизм управления маршрутизацией, механизм нотаризации, физическая или персональная защита, надежное аппаратное/программное обеспечение.

МИРОТВОРЧЕСКИЕ ДЕЙСТВИЯ – совокупность согласованных и взаимосвязанных по целям, задачам, месту и времени одновременных и последовательных действий, проводимых в ограниченном районе специально создаваемой группировкой многонациональных (коалиционных) сил в соответствии с мандатом, утвержденном Советом Безопасности ООН или другим органом коллективной безопасности, в целях создания условий, способствующих политическому разрешению противоречий и исключения возникновения, вооруженного конфликта или его прекращения.

МНОГОУРОВНЕВАЯ ЗАЩИТА - защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

МОДЕЛЬ ЗАЩИТЫ - абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа.

МОДЕЛЬ УГРОЗ – вербальное или формальное описание процесса возникновения угрозы (ее источника), способа воздействия на защищаемые ИР с использованием уязвимостей изделия ИТ и результатов действия угрозы, связанных с нарушением правил ИБ.

НАРУШЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ - нарушение средств управления специфической частью системы информационной, отвечающей за контроль целостности информации и доступа к системе. Может быть как преднамеренное в результате неправомерных действий злоумышленника, так и в результате сбоя в работе отдельных программ или технических компонентов системы. В любом случае следствием является облегчение доступа к информации или информации нарушение в результате неверной (неконтролируемой) работы программного обеспечения защиты данных от изменений.

НАРУШЕНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ - успешное поражение средства управления безопасностью, которое завершается проникновением в систему. Нарушение средств управления специфической информационной системы, как правило, приводит к тому, что информационные активы или компоненты системы становятся доступны неуполномоченным на то лицам или программно-техническим средствам.

НАСТУПАТЕЛЬНЫЕ ИНФОРМАЦИОННЫЕ ОПЕРАЦИИ - единое использование приданных и поддерживающих возможностей и действий, поддерживаемых на взаимной основе разведкой, для оказания воздействия на руководство противника в целях достижения или развития конкретных задач. Эти возможности и действия включают, но не ограничиваются, обеспечением секретности операций, военным введением в заблуждение, психологическими операциями, операциями РЭБ. физическим нападением и/или уничтожением и специальными информационными операциями, а также могут включать нападение на компьютерную сеть.

НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ РОССИЙСКОЙ ФЕДЕРАЦИИ - безопасность многонационального народа как носителя суверенитета и единственного источника власти в РФ.

НАЦИОНАЛЬНЫЕ ИНТЕРЕСЫ РОССИИ В ИНФОРМАЦИОННОЙ СФЕРЕ, соблюдение

конституционных прав и свобод граждан в области получения информации и пользования ею, развитие современных телекоммуникационных технологий, защита государственных информационных ресурсов от несанкционированного доступа.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере:

- соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;
- информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам;
- развитие современных информационных технологий, отечественной индустрии информации, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. На этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности;
- защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

НЕПРАВОМОЧНЫЕ ДЕЙСТВИЯ - действия в отношении ресурса информационного, совершаемые в нарушение правил и полномочий (санкций), установленных для данного ресурса.

НЕПРЕДНАМЕРЕННОЕ ВОЗДЕЙСТВИЕ НА ИНФОРМАЦИЮ - ошибка пользователя информацией, сбой технических и программных средств информационных систем, природные явления или иные нецеленаправленные на изменение информации действия, приводящие к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

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

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП - нарушение регламентированного доступа к объекту защиты.

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ - 1) доступ к информации или ее носителям с нарушением правил доступа к ним. Получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. *К основным способам несанкционированного доступа относятся:*

- непосредственное обращение к объектам доступа;
- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая осуществить несанкционированный доступ;
- внедрение в технические средства средств вычислительной техники или автоматизированной системы программных или технических механизмов, нарушающих предполагаемую структуру и функции средства вычислительной техники или автоматизированной системы и позволяющих осуществить несанкционированный доступ;

2) неправомерный доступ к источникам конфиденциальной информации лицами, не имеющими права доступа к ним. Основными способами НСД являются: сотрудничество, выведывание,

подслушивание, наблюдение, хищение, копирование, подделка, уничтожение, перехват, фотографирование и др..

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ПРОГРАММНЫМ СРЕДСТВАМ - доступ к программам, записанным в памяти ЭВМ или на машинном носителе, а также отраженным в документации на эти программы, осуществленный с нарушением установленных правил.

НОСИТЕЛЬ ИНФОРМАЦИИ - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИТ - система мер по предотвращению или нейтрализации действия угроз безопасности и осуществление предписанной политики безопасности при создании, оценке и в процессе эксплуатации изделий ИТ.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ - реализация конституционных прав и свобод граждан РФ в сфере информационной деятельности; совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство; противодействие угрозе развязывания противоборства в информационной сфере.

Государственная политика обеспечения информационной безопасности Российской Федерацией определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Методы обеспечения информационной безопасности РФ — правовые, организационно-технические и экономические. Правовые методы - разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации. Организационно-технические методы: создание и совершенствование системы обеспечения информационной безопасности РФ; усиление правоприменительной деятельности федеральных органов исполнительной власти субъектов РФ, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере; разработка, использование и совершенствование средств зашиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения; создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи; выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации,; сертификация средств защиты информации, лицензирование деятельности в области зашиты государственной тайны, стандартизация способов и средств защиты информации; совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности; контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации; формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы: разработка программ обеспечения ИБ РФ и определение порядка их финансирования; совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы

страхования информационных рисков физических и юридических лиц. *Цели обеспечения* ИБ страны: соблюдение конституционных прав и свобод граждан в области духовной жизни и информационной деятельности, обеспечение духовного обновления России; развитие отечественной индустрии средств информатизации, телекоммуникаций и связи. обеспечение ею потребностей внутреннего рынка, выхода ее продукции на мировые рынки, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов; обеспечение безопасности информационных ресурсов, информационных и телекоммуникационных систем как развернутых, так и создаваемых на территории России.

Направления обеспечения ИБ — организационное, нормативно-правовое, технологическое, кадровое.

Организационное обеспечение ИБ — безопасности - упорядоченная по полномочиям и взаимодействию и установленная законом совокупность субъектов обеспечения информационной безопасности РФ.

Нормативно-правовое обеспечение ИБ — совокупность правовых норм, регулирующих отношения в области противодействия угрозам информационной безопасности РФ, и установленных государством механизмов реализации этих норм.

Технологическое обеспечение ИБ — совокупность методического обеспечения и технологического инструментария, используемых субъектами обеспечения информационной безопасности РФ в интересах выполнения возложенных на них функций по противодействию угрозам этой безопасности.

Кадровое обеспечение ИБ — система подготовки, переподготовки и использования кадров в интересах субъектов обеспечения ИБ.

ОБЕСПЕЧЕНИЕ СЕКРЕТНОСТИ ИНФОРМАЦИИ - охрана и защита информации и систем информационных от несанкционированного доступа или от изменения информации во время ее хранения, обработки или передачи, а также против воспрещения обслуживания имеющих допуск пользователей. Обеспечение секретности информации включает меры, необходимые для обнаружения, документирования и противодействия таким угрозам. Обеспечение секретности информации состоит из безопасности компьютерной и связи безопасности.

ОБНАРУЖЕНИЕ ВТОРЖЕНИЯ - 1) фиксация факта вторжения, в том числе вторжения электромагнитного по каким-либо признакам; 2) процесс (действия) определения признаков, дающих основание сделать заключение о совершении вторжения, в том числе вторжения электромагнитного.

ОБНАРУЖЕНИЕ МАНИПУЛЯЦИИ - механизм, используемый для обнаружения возможной модификации блока данных (случайной или преднамеренной).

ОБОРОНИТЕЛЬНЫЕ ИНФОРМАЦИОННЫЕ ОПЕРАЦИИ – интеграция и координация политики, методик, операций, личного состава и технологии в целях охраны и защиты информации и информационных систем. Оборонительные информационные операции осуществляются посредством гарантий информационных, обеспечения физической безопасности, оперативной безопасности, контрдезинформации, контрпсихологических операций, контрразведки, РЭБ и информационных операций специальных. Операции информационные оборонительные обеспечивают своевременный, четкий и соответствующий доступ к информации, в то же время не давая противнику возможности использовать свою информацию и информационные системы в своих целях.

ОБОСНОВАННОСТЬ ЗАСЕКРЕЧИВАНИЯ СВЕДЕНИЙ - установление путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экологических или иных последствий этого акта, исходя из баланса жизненно важных интересов государства, общества и граждан.

ОБРАБОТКА ИНФОРМАЦИИ - совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией.

ОБРАТНАЯ СВЯЗЬ (в псих. безоп.) - элемент структуры психологического воздействия, осуществляемый путем учета субъектом воздействия реакции объекта (группы объектов) на информационно-психологическое воздействие и корректировки воздействия на основе данной реакции.

ОБЩИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - общие методы обеспечения информационной безопасности разделяются на правовые, организационно-технические и экономические.

ОБЪЕКТ ДОСТУПА (ОБЪЕКТ) - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

ОБЪЕКТ ИНФОРМАТИЗАЦИИ - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

ОБЪЕКТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - лицо, организация, информационный ресурс, средства и система передачи, приема, обработки и отображения информации в различных системах разведки, управления и сферах деятельности.
Объектами обеспечения ИБ в сфере обороны являются:

- информационная инфраструктура центральных органов военного управления и органов военного управления видов и родов войск, объединений, соединений, воинских частей и организаций, входящих в ВС, научно-исследовательских учреждений Министерства обороны РФ;
- информационные ресурсы предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные заказы либо занимающихся оборонной проблематикой;
- программно-технические средства АСУ войсками (силами) и оружием, вооружения и военной техники, оснащенных средствами информатизации;
- информационные ресурсы, системы связи и информационная инфраструктура других войск, воинских формирований и органов.
- *К основным объектам обеспечения ИБ в сфере внешней политики относятся:*
- информационные ресурсы органов исполнительной власти, реализующих внешнюю политику РФ, российских представительств и организаций за рубежом, представительств при международных организациях;
- информационные ресурсы представительств органов власти, реализующих внешнюю политику РФ, на территориях субъектов РФ;
- информационные ресурсы российских предприятий, учреждений и организаций, реализующие внешнюю политику РФ;
- блокирование деятельности российских средств массовой информации по разъяснению зарубежной аудитории целей и основных направлений государственной политики РФ, ее мнения по социально значимым событиям российской и международной жизни.

ОБЪЕКТ ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ - элемент структуры психологического воздействия, рассматриваемый как человек или определенная совокупность людей (макро или микрогруппа), которая может быть связана или не связана общими целями, ценностями и деятельностью (диффузная группа, ассоциация, корпорация и коллектив), быть или не быть организованной (формальная и неформальная группа), иметь или не иметь постоянные контакты между своими членами (контактная и дистантная группа).

ОБЪЕКТИВНОСТЬ (ИНФОРМАЦИИ) - свойство информации, определяющее ее соответствие реальным описываемым с ее помощью объектам, процессам, явлениям.

ОРГАН ЗАЩИТЫ ИНФОРМАЦИИ - административный орган, осуществляющий организацию защиты информации.

ОРГАНИЗАЦИИ ТЕЛЕ-, РАДИОВЕЩАНИЯ (ТЕЛЕРАДИОВЕЩАТЕЛЬНАЯ КОМПАНИЯ - ТРК) - организация, осуществляющая производство, монтаж, расстановку во времени и распространение с использованием электромагнитных волн (по эфирным, кабельным, проводным и иным электромагнитным системам) звуковой (радиовещание), визуальной и аудиовизуальной (телевещание) массовой информации и данных, предназначенных для получения непосредственно телезрителями и радиослушателями.

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - совокупность приемов, мероприятий и операций, применяемых в информационных технических средствах и системах информатизации организационно-техническими методам обеспечения ИБ относят:

- создание и совершенствование системы ИБ;
- усиление правоприменительной деятельности органов власти, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;
- разработка, использование и совершенствование средств ЗИ и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;
- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств ЗИ при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по ЗИ;
- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств ЗИ;
- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;
- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения ИБ;
- формирование системы мониторинга показателей и характеристик ИБ в наиболее важных сферах жизни и деятельности общества и государства.

ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ ПО ЗИ - мероприятия по ЗИ, предусматривающие установление временных, территориальных и пространственных ограничений на условия использования и режима работы объекта защиты.

ОРГАНИЗАЦИОННЫЙ КОНТРОЛЬ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ - проверка соответствия полноты и обоснованности мероприятий по защите информации требованиям нормативных документов в области защиты информации.

ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ - содержание и порядок действий, направленных на обеспечение защиты информации.

ОСНОВНОЙ СУБЪЕКТ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ - государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной властей.

ОСНОВНЫЕ ВИДЫ ВТОРЖЕНИЙ - некоторыми видами вторжений являются: маскирование, воспроизведение, модификация сообщений, отклонение услуги, внутренние вторжения, внешние вторжения, «лазейка», «троянский конь».

ОСНОВНЫЕ ОБЪЕКТЫ БЕЗОПАСНОСТИ: личность — ее права и свободы; общество — его материальные и духовные ценности; государство — его конституционный строй, суверенитет и территориальная целостность.

ОСНОВНЫЕ СПОСОБЫ ВЕДЕНИЯ ИНФОРМАЦИОННЫХ ОПЕРАЦИЙ – воздействия на информационные объекты противостоящей стороны выделенным составом сил и средств информационного противоборства при обеспечении комплексной защиты своих объектов, осуществляемых одновременно, последовательно и комплексно с поэтапным наращиванием интенсивности и привлекаемых сил.

ОТНЕСЕНИЕ СВЕДЕНИЙ К ГОСУДАРСТВЕННОЙ ТАЙНЕ И ИХ ЗАСЕКРЕЧИВАНИЕ - введение в предусмотренном законом «О государственной тайне» порядке для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям.

ОХРАНЯЕМЫЕ СВЕДЕНИЯ - сведения, составляющие государственную или иную охраняемую законом тайну; 1) сведения о войсках (силах) и их деятельности, определяемые в соответствии с замыслом и задачами стратегической (оперативной, тактической) маскировки; 2) параметры (характеристики) вооружения, военной техники и военных объектов, подлежащие защите от ТСР; 3) секретная информация, циркулирующая в технических средствах передачи информации. Охраняемые сведения, в зависимости от важности объекта защиты, имеют гриф не ниже «секретно».

ПАРАЗИТНОЕ ИЗЛУЧЕНИЕ (ПИ) - побочное излучение, возникающее в результате самовозбуждения электронного устройства из-за паразитных связей в генераторных и усилительных приборах или каскадах. ПИ ведет к образованию неконтролируемого канала утечки информации.

ПАРОЛИРОВАНИЕ (в радиосвязи) - мероприятие имитозащиты, заключающееся в передаче (приеме) корреспондентами радиолинии формализованных сообщений паролей в целях взаимного опознавания корреспондентов в радиолинии.

ПАРОЛЬ - 1) конфиденциальная информация аутентификации, обычно состоящая из строки знаков; 2) идентификатор субъекта доступа, который является его (субъекта) секретом.

ПАССИВНАЯ ПРЕДНАМЕРЕННАЯ РАДИОЭЛЕКТРОННАЯ ПОМЕХА (ПАССИВНАЯ ПОМЕХА) -помеха, создаваемая отражаемым излучением подавляемого РЭС или формированием в среде распространения этого излучения поглощающих, рассеивающих, модулирующих образований.

ПАССИВНАЯ УГРОЗА - угроза несанкционированного раскрытия информации без изменения состояния системы. К пассивным угрозам относятся те, которые при их реализации не приводят к какой-либо модификации любой информации, содержащейся в системе(ах), и где работа и состояние системы не изменяются. Одной из реализаций пассивной угрозы является использование перехвата для анализа информации, передаваемой по каналам связи.

ПАССИВНОЕ СРЕДСТВО ЗАЩИТЫ - средство, обеспечивающее закрытие объекта защиты путем поглощения, отражения или рассеивания излучений объекта.

ПЕРЕДАЮЩИЙ ЦЕНТР (ПЦ) - радиотелевизионные передающие центры (РТПЦ), радиоцентры (РЦ) и иные организации электросвязи, предоставляющие в том числе услуги по распространению теле- и (или) радиопрограмм, подготовленных организациями теле-, радиовещания.

ПЕРЕЧЕНЬ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ - совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

ПЕРИОДИЧЕСКОЕ ПЕЧАТНОЕ ИЗДАНИЕ - газета, журнал, альманах, бюллетень иное издание, имеющее постоянное название, текущий номер и выходящее в свет не реже одного раза в год.

ПОБОЧНОЕ РАДИОИЗЛУЧЕНИЕ - нежелательное РИ, возникающее в результате любых нелинейных процессов в радиопередающем устройстве, кроме процесса манипуляции.

ПОБОЧНЫЕ ЭЛЕКТРОМАГНИТНЫЕ ИЗЛУЧЕНИЯ И НАВОДКИ - 1) электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания; 2) нежелательные излучения и наводки, проявляющиеся в виде побочных, внеполосных, шумовых и наводимых сигналов, потенциально образующих неконтролируемые каналы утечки конфиденциальной информации.

ПОБОЧНЫЙ КАНАЛ ПРИЕМА - в радиоприемнике, полоса частот, находящаяся за пределами основного канала радиоприемника (как правило, в области высших гармоник), в которой сигнал и/или помеха проходят на выход радиоприемника.

ПОКАЗАТЕЛЬ ЗАЩИЩЕННОСТИ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ - характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники.

ПОКАЗАТЕЛЬ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ - мера или характеристика для оценки эффективности ЗИ.

ПОЛУЧЕНИЕ (ДОБЫВАНИЕ) ИНФОРМАЦИИ - действия, связанные со сбором, обработкой и анализом фактов, связанных со структурой, свойствами и взаимодействием объектов и явлений, извлекаемых из поступающих сигналов и знаков.

ПОМЕХИ - обширная область явлений, препятствующих нормальной работе аппаратуры, устройств комплексов и вызывающих отклонение от расчетных (номинальных) значений параметров работы различных технических средств. Затрудняют обнаружение, определение координат, распознавание, селекцию и сопровождение целей, а также связь, передачу данных и т п. По источнику возникновения помехи делятся на искусственные и естественные. По физическим полям различают помехи электрические, магнитные, электромагнитные, включая тепловые в инфракрасном диапазоне волн, акустические (в том числе гидроакустические), гравитационные и вибрационные.

ПОМЕХОЗАЩИЩЕННОСТЬ - показатель эффективности комплекса мер, направленных на обеспечение надежности работы технических устройств (комплексов) в условиях помех.

ПОМЕХОЗАЩИЩЕННОСТЬ СИСТЕМЫ ВОЕННОЙ СВЯЗИ - способность систем военной связи обеспечивать управление войсками (силами) и оружием в условиях воздействия преднамеренных помех противника.

ПОМЕХОУСТОЙЧИВОСТЬ (ПУ) - 1) характеризует способность радиоэлектронных средств и систем работать с требуемым качеством при воздействии помех. Ее оценивают вероятностью выполнения РЭС (системой) задач в условиях преднамеренных или непреднамеренных помех. Например, ПУ РЛС часто характеризуют вероятностью правильного обнаружения сигналов, отраженных от целей. Требования к ПУ отличаются большим разнообразием в зависимости от допустимых искажений принимаемых сигналов (информации). Так, в некоторых системах передачи данных, использующих ЭВМ, допускается искажение не более одного знака на миллион переданных, в то время как РЛС иногда могут выполнять свои функции при потере до 40% сигналов, отраженных целей.

К техническим способам и средствам ПУ относят также такие, которые реализуются в принципах построения радиоэлектронных средств и систем, в способах передачи, приема и

обработки сигналов, в схемах защиты от помех. Их реализация основана на учете различных полезных сигналов РЭС от радиопомех в несущей частоте, амплитуде, фазе, длительности. частоте следования, направлении прихода, поляризации и положении фазового фронта электромагнитных волн в месте приема, а также случайных изменений перечисленных параметров.

Техническими средствами и способами защиты от помех являются: получение необходимого отношения сигнал/помеха в приемнике РЭС; накопление сигналов в радиоприемном устройстве; предотвращение перегрузки приемных устройств; селекция (выделение и фильтрация сигналов; помехоустойчивое кодирование; использование излучений средств помех для получения информации о целях и др.

В перспективе возможно применение оптимальных способов приема и самонаправляющихся (адаптивных) систем, способных на основе анализа помех и качества приемы изменять параметры сигналов и характеристики приемных устройств, с тем чтобы свести к минимуму эффект воздействия помех на РЭС.

Необходимое превышение полезного сигнала над помехой в месте приема на входе или в тракте приемника можно получить увеличением энергетического потенциала РЭС и накоплением в них сигналов;

2) способность технического устройства выполнять свои функции с требуемым качеством в условиях воздействия помех.

ПОРАЖЕНИЕ СРЕДСТВАМИ СПЕЦИАЛЬНОГО ПРОГРАММНО-ТЕХНИЧЕСКОГО ВОЗДЕЙСТВИЯ - разрушение (искажение) программного обеспечения и баз данных (знаний) путем внедрения в автоматизированные системы специальных программ (вирусов).

ПОРАЖЕНИЕ ЭЛЕКТРОМАГНИТНЫМ ИЗЛУЧЕНИЕМ - функциональное поражение, заключающееся в разрушении (повреждении) элементов и узлов радиоэлектронных объектов противника мощными излучениями.

ПРАВИЛА РАЗГРАНИЧЕНИЯ ДОСТУПА - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

ПРАВО ДОСТУПА К ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ - совокупность правил доступа к защищаемой информации, установленных правовыми документами или собственником, владельцем информации.

ПРАВО ИНФОРМАЦИОННОЕ - совокупность законодательных информационно-правовых норм, регулирующих общественные отношения в информационной сфере и являющихся гарантированным инструментом охраны интеллектуальной информационной собственности (информационного продукта) юридических и физических лиц.

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИБ - нормативные правовые акты, регламентирующие отношения в информационной сфере, и нормативные методические документы по обеспечению ИБ.

ПРЕДНАМЕРЕННАЯ РАДИОЭЛЕКТРОННАЯ ПОМЕХА (ПРЕДНАМЕРЕННАЯ ПОМЕХА) - специально создаваемая помеха для снижения эффективности функционирования РЭС. В зависимости от диапазона, в котором создается преднамеренная помеха, различают радиопомехи, оптико-электронные помехи и акустические помехи.

ПРЕДПОСЫЛКИ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА - совокупность факторов, создающих благоприятные условия для доступа несанкционированного.

ПРЕСС-КОНФЕРЕНЦИЯ, ИНТЕРВЬЮ [при ведении предвыборной агитации] - не являющиеся политической рекламой обращения кандидата (кандидатов), их доверенных лиц, представителя (представителей) избирательных объединений к избирателям с изложением собственной предвыборной программы (платформы), сообщения, сделанные в ходе встречи с журналистом (журналистами).

ПРИГОДНОСТЬ (ГОТОВНОСТЬ) ИНФОРМАЦИИ - обеспечение способности системы

продолжать работать эффективно и поддерживать доступность информации. Принцип, который гарантирует, что система и данные работают и доступны пользователям. В этом контексте отказ от обслуживания рассматривается как нападение на пригодность (готовность) информации.

ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ: законность; соблюдение баланса жизненно важных интересов личности, общества и государства; взаимная ответственность личности, общества и государства по обеспечению безопасности; интеграция с международными системами безопасности.

ПРОВЕРКА БЕЗОПАСНОСТИ - независимый просмотр, изучение системных журналов и наблюдение за функционированием с целью определения достаточности средств контроля системы, соответствия принятой методике безопасности и процедурам обработки данных, обнаружения нарушений безопасности, выработки рекомендаций по изменению средств контроля и процедур безопасности.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ - совокупность программ на носителях данных и программных документов, предназначенная для отладки, функционирования и проверки работоспособности автоматизированной системы.

ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ - системы защиты компьютера от чужого вторжения. Программные средства защиты весьма разнообразны и могут быть классифицированы на такие группы, как:

- средства собственной защиты, предусмотренные общим программным обеспечением;
- средства защиты в составе вычислительной системы;
- средства защиты с запросом информации;
- средства активной защиты;
- средства пассивной защиты и др.

Можно выделить следующие направления использования программ для обеспечения безопасности конфиденциальной информации:

- защита информации от несанкционированного доступа;
- защита информации от копирования;
- защита программ от копирования;
- защита программ от вирусов; защита информации от вирусов;
- программная защита каналов связи.

ПРОПАГАНДА - 1) любая форма распространения информации в поддержку заданных целей, рассчитанная на влияние на мнения, эмоции, отношения или поведение отдельных индивидов или групп, в том числе социальных; 2) форма информационно-психологического воздействия, основанная на воздействии на сознание (подсознание), политические и ценностные ориентации объектов (групп объектов) психологической борьбы посредством распространения воззрений, идей, учений с целью формирования мировоззрения, соответствующего интересам государства.

ПРОТИВОДЕЙСТВИЕ РАЗВЕДКЕ ПРОТИВНИКА - совокупность мер, направленных на создание условий, в которых использование противником сил и средств разведки становится невозможным или неэффективным и заключается: в выявлении и поражении сил и средств разведки, пунктов управления разведкой; в противодействии ТСР противника; в организации борьбы с воздушной разведкой и с диверсионно-разведывательными группами противника.

ПРОТИВОРАДИОЛОКАЦИОННЫЙ ПАТРОН (СНАРЯД) - патрон (снаряд), снаряженный противорадиолокационными отражателями.

ПСИХОЛОГИЧЕСКАЯ БОРЬБА - 1) негативное воздействие на людей с целью изменения в желаемом направлении психологических характеристик (взглядов, мнений, ценностных ориентации, настроений мотивов, установок, стереотипов поведения), а также групповых норм, массовых настроений общественного сознания в целом, проводимая специальными органами (аппаратом) одного государства ради достижения своих политических, а также чисто военных

целей; 2) содержание деятельности специальных органов (аппарата) одного государства, оказывающих психологическое воздействие на гражданское население и (или) на военнослужащих другого государства ради достижения своих политических, а также чисто военных целей.

ПСИХОЛОГИЧЕСКАЯ ВОЙНА - 1) использование пропаганды и других психологических действий, имеющих первичную цель влияния на мнения, эмоции, отношения, и поведение отдельных личностей, групп людей и население противника таким способом, чтобы поддержать достижение целей войны; 2) действия психологические, направленные на решение политических, военных, экономических и идеологических задач с целью создавать в отношении враждебного государства эмоции, отношения или поведение, способствующие достижению своих целей.

ПСИХОЛОГИЧЕСКИЕ ДЕЙСТВИЯ - запланированные действия, направленные на доведение специально отобранной информации потребителю (конкретным субъектам, группам, населению) с тем, чтобы повлиять на его эмоции, поводы, цели, рассуждения и в конечном счете поведение противника (его правительства, организаций, групп и индивидуумов). Вспомогательная цель может состоять в том, чтобы стимулировать или укрепить у противника отношения и поведение, благоприятные для целей субъекта действия психологического. Синоним: операции психологические.

ПСИХОЛОГИЧЕСКИЕ ДЕЙСТВИЯ СТРАТЕГИЧЕСКИЕ - действия психологические, проводимые с широкими или долгосрочными целями в координации с общим стратегическим планированием, с постепенными результатами, осуществимыми в будущем. Направлены на руководящие круги, командование, личный состав вооруженных сил и гражданское население противника в его тылу или прифронтовой полосе позади боевых зон или на аналогичные круги дружественных противнику или нейтральных стран.

ПСИХОЛОГИЧЕСКОЕ ВОЗДЕЙСТВИЕ - определенная социальная активность одних людей, осуществляемая в различных формах и различными средствами (в том числе и непсихологическими), направленная на других людей и их группы с целью изменения и: поведения и деятельности посредством влияния на их взгляды, мнения, отношения ценностные ориентации, мотивы, установки и стереотипы, настроения (их психику и сознание).

ПСИХОЛОГИЧЕСКОЕ ВОЗДЕЙСТВИЕ НА ВОЙСКА И НАСЕЛЕНИЕ ЗАРУБЕЖНЫХ СТРАН (ПРОТИВНИКА) - такое воздействие на индивидуальное и общественное сознание военными, пропагандистскими, психологическими или иными способами и средствами, которое вызывает трансформацию их психики, способствует снижению морального духа, заставляет прекращать боевые действия и сопротивление в условиях современной войны.

ПСИХОТРОННОЕ ОРУЖИЕ – средства воздействия на психику и подсознание человека с целью снижения его воли, подавление, временный вывод из строя, зомбирование.

ПСИХОТРОННЫЕ СРЕДСТВА - технические информационные средства (акустические, визуальные, лазерные, электромагнитные, генераторы неизвестных излучений и т.д.) воздействия на человека с целью модификации его психики (в основном через подсознание) в нужном для воздействующей стороны направлении. ПС составляют техническую часть психофизического оружия.

ПСИХОТРОПНОЕ ОРУЖИЕ – специально структурированные лекарства, психофармакологические и психодислептические препараты, транквилизаторы, антидепрессанты, галюциногены, наркотики, алкогольные компоненты и др. средства, предназначенные для воздействия на психику отдельного человека или компактной группы людей.

ПСИХОТРОПНЫЕ СРЕДСТВА - специально структурированные лекарства, психофармакологические и психодислептические препараты, транквилизаторы, антидепрессанты, галлюциногены, наркотики, алкогольные компоненты и т.п. средства, предназначенные для воздействия на психику (в основном через подсознание) отдельного человека или группы людей с целью модификации ее в нужном для воздействующей стороны направлении.

ПУНКТ УПРАВЛЕНИЯ КОМПЛЕКСА РАДИОЭЛЕКТРОННОГО ПОДАВЛЕНИЯ - совокупность технических устройств, предназначенных для сбора, обработки, отображения, хранения передачи и документирования информации и обеспечивающих управление комплексом РЭП.

РАДИОЗАКЛАДКА - миниатюрное электронное устройство, состоящее из микрофона и миниатюрного радиопередатчика, обеспечивающего передачу подслушивающего передачу подслушиваемых переговоров на достаточно значительное расстояние с помощью электромагнитных волн. Радиозакладки камуфлируются под бытовые и технические приборы, как составные элементы мебели, оборудования офисов и служебных кабинетов.

РАДИОКОНТРОЛЬ - наблюдение за установленным порядком работы радиоэлектронных средств в целях проверки выполнения требований защиты информации, мер радиомаскировки, соблюдения норм на ПЭМИН. Осуществляется с помощью пунктов радиоконтроля.

РАДИОМАСКИРОВКА - комплекс организационных и технических мероприятий, направленных на снижение эффективности радиоразведки. Достигается ограничением времени работы своих радиостанций на передачу, уменьшением мощности излучений, использованием направленных антенн, применением аппаратуры быстродействия, созданием ложных радиосетей и радионаправлений и другими методами.

РАДИООТРАЖАТЕЛЬ - устройство, обеспечивающее отражение радиоволн «обратно» в точку (среду) их излучения.

РАДИОПЕРЕХВАТ - 1) перехват радиосообщений, в которых возможно выделить элементы смысловой информации: заголовки радиограмм, настроечных текстов, пусковых комбинаций линейного шифрования, участков текста передач и т.п.; 2) обнаружение, прием и регистрация радиоизлучений в целях последующего вскрытия содержания передач или выявление группировки объектов по работающим радиостанциям; способ ведения радиоразведки.

РАДИОПОДАВЛЕНИЕ - преднамеренное подавляющее или маскирующее воздействие энергией радиоволн на РЭС, работающие в радиодиапазоне электромагнитных волн.

РАДИОРАЗВЕДКА - 1) добывание радиоразведывательных данных о противнике по излучениям его РЭС; 2) добывание сведений путем приема радиоизлучений средств радиосвязи, телеметрии, информатики и оргтехники, их анализа и восстановления передаваемых сообщений.

РАДИОЭЛЕКТРОННАЯ БОРЬБА (РЭБ) - 1) одна из форм борьбы в войне, заключающаяся в радиоэлектронном поражении противника и радиоэлектронной защите своих войск; 2) совокупность согласованных мероприятий и действий войск (сил) по радиоэлектронному поражению противника и радиоэлектронной защите своих войск (сил).

РАДИОЭЛЕКТРОННАЯ ЗАЩИТА - 1) устранение (ослабление) воздействия на радиоэлектронные объекты средств радиоэлектронного поражения противника, защите от непреднамеренных взаимных радиопомех и от средств радиоэлектронной разведки противника. Р.з. включает: защиту от радиоэлектронного поражения противника, защиту от непосредственных радиопомех, скрытие от радиоэлектронной разведки противника; 2) комплекс мероприятий по обеспечению устойчивой работы радиоэлектронных средств и систем от их подавления, поражения, нарушения их работы, несанкционированного подслушивания и исключения возникновения неконтролируемых каналов за счет ПЭМИН; 3) устранение или ослабление воздействия на РЭС оружие, военную технику и объекты средств радиоэлектронного подавления противника и взаимных радиоэлектронных помех проводится с целью обеспечения устойчивости функционирования систем управления, разведки, наведения оружия. РЭЗ включает защиту от радиоэлектронного подавления поражения управляемым оружием, обеспечения электромагнитной совместимости, а также защиту РЭС от естественных радиоэлектронных помех. Объектами РЭЗ являются РЭС, системы управления войсками (силами), оружием и объектами. Достигается проведением организационных, технических мероприятий, обеспечением помехоустойчивости, а также специальной подготовкой их операторов, систем наведения оружия, личного состава, узлов связи, пунктов управления войсками (силами), оружием и объектами.

РАДИОЭЛЕКТРОННАЯ РАЗВЕДКА - 1) добывание данных о составе, состоянии, местоположении, режимах работы и характеристиках сигналов, излучаемых радиоэлектронными средствами противника, необходимых для организации и ведения радиоэлектронной борьбы, на основе приема и анализа электромагнитных, акустических (в водной среде) излучений. Различают общую и непосредственную (исполнительную) разведку. По видам используемых средств различают радиолокационную, оптико-электронную и акустическую разведки; 2) добывание сведений о противнике с помощью радиоэлектронных средств. Подразделяется на радиоразведку, радиотехническую, радиолокационную, радиотепловую (тепловизионная), тепловую (инфракрасная), лазерную, телевизионную, звуковую, гидроакустическую разведку.

РАДИОЭЛЕКТРОННОЕ ПОДАВЛЕНИЕ - 1) подавляющее воздействие на радиоэлектронные объекты противника энергией электромагнитных (акустических) излучений; 2) нарушение работы или снижение эффективности применения средств радиоэлектронной разведки путем воздействия на них средствами РЭП.

РАДИОЭЛЕКТРОННОЕ ПОРАЖЕНИЕ - поражающее воздействие на радиоэлектронные объекты электромагнитной (акустической) и кинетической энергией, а также изменение условий распространения (отражения) электромагнитных (акустических) волн. Радиоэлектронное поражение включает: функциональное поражение, радиоэлектронное подавление, поражение самонаводящимся на излучение оружием и изменение условий распространения электромагнитных (акустических) волн.

РАДИОЭЛЕКТРОННО-ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ - совокупность мероприятий выявления и контроля функционирования радиоэлектронных объектов, сбор, анализ и обобщение данных о радиоэлектронной обстановке, необходимых для организации радиоэлектронного поражения и радиоэлектронной разведки.

РАДИОЭЛЕКТРОННЫЕ ПОМЕХИ (РП) - 1) мешающее или подавляющее воздействие энергии электромагнитных и акустических излучений, которое ухудшает или может ухудшить качество функционирования радиоэлектронных средств (РЭС); вид помех в технике. В результате воздействия Р.П. затрудняется или исключается прием или выделение полезных сигналов, передача информации, обнаружение целей и наблюдений за ними, навигация и выход в район целей самолетов, кораблей, танков и другой боевой техники, пуск (стрельба) и наведение боеприпасов, снижается их боевая эффективность; 2) непоражающие электромагнитные (акустические) излучения, которые ухудшают качество функционирования РЭС, оружия и военной техники; мешающее воздействие энергии электромагнитных и акустических излучений, которые ухудшают показатели качества функционирования РЭС.

РАДИОЭЛЕКТРОННЫЕ СРЕДСТВА - 1) технические средства, состоящие из одного или

нескольких радиопередающих или радиоприемных устройств или их комбинации и вспомогательного оборудования, предназначенные для передачи и приема радиоволн; 2) радиостанции, радиотелефоны, системы радионавигации, радио-определения, системы кабельного телевидения и другие устройства, при работе которых используются электромагнитные колебания с частотами выше 9 кГц.

РАЗВЕДЫВАТЕЛЬНАЯ ДЕЯТЕЛЬНОСТЬ - деятельность, которая осуществляется органами внешней разведки Российской Федерации посредством добывания и обработки информации о затрагивающих жизненно важные интересы Российской Федерации реальных и потенциальных возможностях, действиях, планах и намерениях иностранных государств, организаций и лиц, а также оказание содействия в реализации мер, осуществляемых государством в интересах обеспечения безопасности Российской Федерации.

РАЗВЕДЫВАТЕЛЬНАЯ ИНФОРМАЦИЯ - информация о затрагивающих жизненно важные интересы Российской Федерации реальных и потенциальных возможностях, действиях, планах и намерениях иностранных государств, организаций и лиц.

РАЗГЛАШЕНИЕ ИНФОРМАЦИИ - несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к этой информации.

РАЗРУШЕНИЕ ИНФОРМАЦИИ - полная потеря хранящихся в информационных системах или передаваемых по информационным сетям данных или их изменение, исключающее возможность правильной их интерпретации и восстановления.

РАСПРОСТРАНЕНИЕ СЛУХОВ - прием психологического воздействия в психологической операции, рассматриваемый как распространение, в основном недостоверной информации, выгодной субъекту, организующему и ведущем} психологическую борьбу, как правило, путем широкого привлечения неофициальных каналов (в том числе агентурных) с целью снижения морально-психологического состояния объекта воздействия.

РАССЕКРЕЧИВАНИЕ СВЕДЕНИЙ И ИХ НОСИТЕЛЕЙ - снятие ранее введенных в предусмотренном настоящим Законом порядке ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям.

РАСШИФРОВАНИЕ ДАННЫХ - процесс преобразования зашифрованных данных в открытые при помощи шифра.

РАСШИФРОВКА - действие по получению информации из формы, в которую данные были превращены, чтобы не предоставлять доступа посторонним лицам.

РЕДАКЦИЯ СРЕДСТВА МАССОВОЙ ИНФОРМАЦИИ - организация, учреждение, предприятие либо гражданин, объединение граждан, осуществляющие производство и выпуск средства массовой информации.

РЕЖИМНЫЕ ОБЪЕКТЫ - военные и специальные объекты, воинские части, предприятия, организации, учреждения, для функционирования которых установлены дополнительные меры безопасности.

РЕЖИМЫ ЗАЩИТЫ ИНФОРМАЦИИ - установленный порядок и совокупность правил, мероприятий и норм для обеспечения надежной ЗИ.

Режимы защиты информации устанавливаются: в отношении сведений, отнесенных к государственной тайне, - уполномоченными органами на основании Закона Российской Федерации «О государственной тайне»; в отношении конфиденциальной документированной информации – собственником информационных ресурсов или уполномоченным лицом на основании Федерального закона; в отношении персональных данных – установленные Федеральным законом.

РУБЕЖИ ЗАЩИТЫ ИНФОРМАЦИИ - совокупность методов и средств, обеспечивающая

многоуровневую, иерархическую систему допуска к информации с помощью различных средств, таких как физические, технические, программные и т.п. Иерархическая последовательность доступа к информации реализуется по принципу «чем выше уровень доступа, тем уже круг допущенных лиц».

САМОНАВОДЯЩЕЕСЯ НА ИСТОЧНИК РАДИОИЗЛУЧЕНИЯ ОРУЖИЕ - высокоточное оружие с пассивными радиоэлектронными системами наведения, предназначенное для огневого поражения радиоэлектронных объектов противника.

САНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ - доступ к информации, не нарушающий правил разграничения доступа.

СБОР, АНАЛИЗ И ДОВЕДЕНИЕ ДАННЫХ О РАДИОЭЛЕКТРОННОЙ ОБСТАНОВКЕ - совокупность мероприятий по сбору, накоплению, анализу, хранению и доведению до органов управления радиоэлектронной борьбой данных о радиоэлектронных средствах, системах противника и своих войск, сил, добываемых средствами радиоэлектронной разведки и комплексного радиоэлектронного контроля соединений и частей РЭБ, а также данных, получаемых от других источников, необходимых для организации и ведения РЭБ.

СВЕДЕНИЯ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА - сведения, входящие в следующий перечень:

- сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в СМИ, в установленных федеральными законами случаях;
- сведения, составляющие тайну следствия и судопроизводства;
- служебные сведения, доступ к которым ограничен органами государственной власти (служебная тайна);
- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и так далее);
- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен органами государственной власти;
- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

СВЕДЕНИЯ КРИТИЧЕСКИЕ - сведения, которые требуют непосредственного (немедленного) внимания и реагирования командующего. Включают, но не ограничиваются следующим: явные признаки неизбежной вспышки военных действий любого типа (предупреждение нападения); агрессия любого характера (природы) против дружественной страны; признаки использования ОМУ; существенные признаки в пределах потенциальных вражеских стран, которые могут вести к модификации стратегических планов.

СВЕДЕНИЯ ОСОБОЙ ВАЖНОСТИ - сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам РФ в одной или нескольких из перечисленных областей.

СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ - защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести вред безопасности государства.

СЕКРЕТНАЯ ИНФОРМАЦИЯ - информация, содержащая сведения, отнесенные к государственной тайне.

Не подлежат засекречиванию сведения:

- о ЧС и катастрофах, угрожающих безопасности и здоровью граждан и последствиях, о их официальных прогнозах и последствиях;

– о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
– о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам и организациям;
– о фактах нарушения прав и свобод человека и гражданина;
– о размерах золотого запаса и государственных валютных резервах РФ;
– о состоянии здоровья высших должностных лиц РФ;
– о фактах нарушения законности органами государственной власти и их должностными лицами.

СЕКРЕТНОСТЬ - ограничение, накладываемое собственником, на доступ к информации, документам, делам, базам данных, продукции, оборудованию, транспорту, на вход и нахождение в определенной зоне (территории), здании, помещениях.

СЕТИ ЭЛЕКТРОСВЯЗИ - технологические системы, обеспечивающие один или несколько видов передач: телефонную, телеграфную, факсимильную, передачу данных и других видов документальных сообщений, включая обмен информацией между ЭВМ, телевизионное, звуковое и иные виды радио- и проводного вещания.

СЕТЬ СВЯЗИ - совокупность электрических сетей связи и сетей почтовой связи. Они функционируют как взаимоувязанный производственно-хозяйственный комплекс, предназначенный для удовлетворения нужд граждан, органов государственной власти и управления, обороны, безопасности, охраны правопорядка физических и юридических лиц в услугах электрической и почтовой связи.
Примечание. Сети электрической связи реализуют передачу и прием любых знаков, сигналов, письменного текста, изображений, звуков по проводной, радио-, оптической и другим электромагнитным системам. Системы передачи данных являются разновидностью систем электрической связи, в которых передача информации осуществляется в цифровом виде и на основе специальных протоколов обмена информацией между отправителем и получателем.

СЕТЬ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ - составная часть взаимоувязанной сети связи Российской Федерации, открытая для пользования физическим и юридическим лицам, в услугах которой этим лицам не может быть отказано.

СИСТЕМА ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ - совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ - совокупность органов и(или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ - совокупность технических, программных и программно-технических средств ЗИ и средств контроля ее эффективности.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА - комплекс организационных мер и программно-технических средств защиты от несанкционированного доступа к информации.

СИСТЕМА КОМАНДОВАНИЯ И УПРАВЛЕНИЯ - средства обслуживания, оборудование, коммуникации, процедуры и персонал, необходимый для командующего для планирования, направления и действий управления назначенных сил в соответствии с установленными назначениями.

СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ - совокупность правовых, организационных и

технических мероприятий, норм, служб и механизмов обеспечения безопасности России. Систему безопасности России образуют органы законодательной, исполнительной и судебной властей, государственные, общественные и иные организации и объединения, граждане, принимающие участие в обеспечении безопасности в соответствии с законом, а также законодательство, регулирующее отношения в сфере безопасности.

Основными функциями системы безопасности являются:

- выявление и прогнозирование внутренних и внешних угроз жизненно важным интересам объектов безопасности,
- осуществление комплекса мер по их предупреждению и нейтрализации, создание и поддержание в готовности средств обеспечения безопасности;
- управление силами и средствами обеспечения безопасности в повседневных условиях и в чрезвычайной ситуации;
- осуществление системы мер по восстановлению нормального функционирования объектов безопасности в регионах, пострадавших в результате чрезвычайной ситуации;
- участие в мероприятиях по обеспечению безопасности за пределами РФ в соответствии с международными договорами и соглашениями, заключенными или признанными РФ.

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ - часть системы обеспечения национальной безопасности страны. Основными элементами организационной основы системы обеспечения ИБ РФ являются: Президент Российской Федерации, Совет Федерации Федерального Собрания РФ, Государственная Дума Федерального Собрания РФ, Правительство РФ, Совет Безопасности РФ, федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом РФ и Правительством РФ, органы исполнительной власти субъектов РФ, органы местного самоуправления, органы судебной власти, общественные объединения, граждане, принимающие в соответствии с федеральным законодательством РФ участие в решении задач обеспечения информационной безопасности.

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ СВЯЗИ - совокупность правовых, организационных и технических мероприятий, норм, служб и механизмов защиты, органов управления и исполнителей, направленных на противодействие угрозам ИБ с целью сведения до минимума возможного ущерба пользователю или оператору связи.

СИСТЕМА ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ - органы, силы и средства обеспечения национальной безопасности, осуществляющие меры политического, правового, организационного, экономического, военного и иного характера, направленные на обеспечение безопасности личности, общества и государства.

СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЯ - программное обеспечение и (или) система аппаратных средств ЭВМ, разработанная (предназначенная) для контроля технико-программных средств компьютера, информационной системы или сети с целью идентификации признаков вторжения попытки.

СИСТЕМА ОБРАБОТКИ ИНФОРМАЦИИ - совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, обеспечивающая выполнение автоматизированной обработки информации.

СИСТЕМА ПРЕДУПРЕЖДЕНИЯ И ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК – часть системы обеспечения информационной безопасности информационно-телекоммуникационной системы, предназначенная для обнаружения и идентификации компьютерных атак, определения их источников, выработки и доставки сигналов оповещения в систему принятия ответных мер, а также для проведения комплекса мероприятий по выявлению и устранению возможностей реализации компьютерных атак.

СИСТЕМА РАДИОЭЛЕКТРОННОГО ПОДАВЛЕНИЯ - совокупность комплексов или средств РЭП, объединенных единым алгоритмом функционирования и общим управлением, предназначенных для решения задач радиоэлектронного подавления.

СИСТЕМА РАЗГРАНИЧЕНИЯ ДОСТУПА - совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ - совокупность участников сертификации, осуществляющих ее на основании требований государственных стандартов, нормативных документов, утверждаемых Правительством Российской Федерации и федеральными органами по сертификации в пределах их компетенции.

СИСТЕМА УПРАВЛЕНИЯ ВОЕННОЙ СВЯЗЬЮ - часть системы военной связи, обеспечивающая функционирование системы военной связи с заданным качеством. Состоит из иерархически взаимоувязанных органов и пунктов управления системы военной связи, средств служебной связи и средств автоматизации.

СИСТЕМА ФОРМИРОВАНИЯ И ОБЕСПЕЧЕНИЯ СОХРАННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ - совокупность систем государственных архивных учреждений, информационных фондов органов государственной власти, муниципальных образований, просветительских организаций (в первую очередь, библиотек), частных лиц и организаций, осуществляющих деятельность по сбору, накоплению, хранению, обработке и распространению информации по различным направлениям жизни общества и государства.

СКРЫТНОСТЬ СИСТЕМЫ ВОЕННОЙ СВЯЗИ - способность системы военной связи сохранять в тайне от противника оперативную информацию, передаваемую и хранящуюся в системе военной связи, а также изменения структуры и характера функционирования, связанные с изменениями степени боевой готовности войск (сил) и проведением войсками операций.

СЛУЖБА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЗАИМОУВЯЗАННОЙ СЕТИ СВЯЗИ РОССИЙСКОЙ ФЕДЕРАЦИИ - организационно-техническая структура системы обеспечения информационной безопасности взаимоувязанной сети связи, реализующая решение определенной задачи, направленной на противодействие той или иной угрозе информационной безопасности этой сети.

СЛУЖЕБНАЯ ИНФОРМАЦИЯ - 1) информация, не содержащая сведений, составляющих государственную тайну, определяемая установленными в государстве ведомственными перечнями собственников информации, циркулирующая в органах государственной власти и управления, а также в государственных и коммерческих предприятиях и учреждениях, выполняющих государственные заказы, подлежащая защите (собственником этой информации) от иностранных технических разведок и от ее утечки при передаче по каналам и сетям связи; 2) сведения, появляющиеся в связи с реализацией функций государственной службы. Круг сведений, составляющих информацию служебную, весьма широк и охватывает все сферы деятельности органов государственной власти.

СЛУЖЕБНАЯ ИНФОРМАЦИЯ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ - несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью.

СОВЕРШЕННО СЕКРЕТНЫЕ СВЕДЕНИЯ - к совершенно секретным сведениям относят сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики.

СОВЕТ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ - 1) конституционный орган, осуществляющий подготовку решений Президента РФ в области обеспечения безопасности, рассматривающий вопросы внутренней и внешней политики Российской Федерации в области обеспечения безопасности, стратегические проблемы государственной, экономической, общественной, оборонной, информационной, экологической и иных видов безопасности, охраны здоровья населения, прогнозирования, предотвращения чрезвычайных ситуаций и преодоления их

последствий, обеспечения стабильности и правопорядка; 2) конституционный орган, осуществляющий подготовку решений Президента Российской Федерации по вопросам обеспечения защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, проведения единой государственной политики в области обеспечения безопасности.

СОВМЕСТНАЯ ИНФОРМАЦИОННАЯ ОПЕРАЦИЯ – совокупность согласованных и взаимоувязанных по целям, задачам, направлению (региону) и времени специальных операций, информационных действий, акций и других форм применения сил и средств информационного противоборства, проводимых несколькими органами власти по единому замыслу и плану.

СООБЩЕНИЕ - блок данных, передаваемый средствами передачи и имеющий в составе заголовок и содержательную (информационную) часть.

СПЕЦИАЛИЗИРОВАННОЕ СРЕДСТВО МАССОВОЙ ИНФОРМАЦИИ - такое средство массовой информации, для регистрации или распространения продукции которого настоящим Законом установлены специальные правила.

СПЕЦИАЛЬНЫЕ ВОЗДЕЙСТВИЯ НА ИНФОРМАЦИЮ - воздействия в целях уничтожения, искажения и блокирования информации.

СПЕЦИАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ОПЕРАЦИИ - информационные операции, которые в силу своего секретного характера, их возможного потенциального эффекта или воздействия, соображений безопасности или угрозы национальной безопасности требуют особого процесса рассмотрения и одобрения.

СПЕЦИАЛЬНЫЕ ОБЪЕКТЫ - пункты управления государством и ВС, а также другие объекты, обеспечивающие функционирование федеральных органов государственной власти РФ в военное время.

СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ - порядок и правила применения определенных принципов и средств ЗИ.

СПОСОБ КОНТРОЛЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ - порядок и правила применения определенных принципов и средств контроля эффективности ЗИ.

СПОСОБЫ ДЕЙСТВИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ - выявление возможных каналов утечки информации, поиск и обнаружение реальных каналов утечки информации, оценка степени опасности каждого реального канала, локализации (подавление) опасных каналов и контроль надежности защитных мероприятий.

СПОСОБЫ ИНФОРМАЦИОННОЙ БОРЬБЫ - порядок и приемы применения сил и средств объединения (соединения, части, подразделения) для захвата и удержания информационного превосходства над противником при подготовке и в ходе боевых действий. Способы ИБ включают: вид и последовательность информационных воздействий на противника; объекты воздействий; состав сил и средств, выделяемых для ведения информационной борьбы, их оперативное построение (боевой порядок).

Способы ИБ делятся на три основные категории*: силовые, интеллектуальные и комбинированные.* Кроме того, в ИБ можно выделить две основные группы способов: *наступательные и оборонительные*. Наступательные способы ИБ: блокирование, отвлечение, сковывание, изматывание, инсценировка, дезинтеграция, умиротворение, устрашение, провоцирование, внушение и давление; оборонительные способы ИБ: деблокирование и отождествление.

СПОСОБЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА - приемы и порядок действий с целью получения (добывания) охраняемых сведений незаконным путем. К ним, в том числе, относятся инициативное сотрудничество (предательство, измена), склонение (принуждение, побуждение) к

сотрудничеству (подкуп, шантаж), подслушивание переговоров, незаконное ознакомление, хищение, подделка (модификация), уничтожение (порча, разрушение), незаконное подключение к системам и линиям связи и передачи информации; перехват акустических и электромагнитных сигналов, визуальное наблюдение, фотографирование, сбор и анализ документов, публикаций и промышленных отходов.

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ - 1) технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности ЗИ; 2) технические средства, используемые для формирования. обработки, передачи или приема сообщений электросвязи либо почтовых отправлений; 3) технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную (коммерческую) тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

СРЕДСТВА ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА - программные, технические или программно-технические средства, предназначенные для предотвращения или существенного затруднения несанкционированного доступа.

СРЕДСТВА ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ - 1) совокупность специальных лингвистических, программных, технических и иных средств, обеспечивающих внедрение**,** извлечение, искажение или разрушение информации, потоков информационных или ресурсов информационных; 2) в информационных операциях эффективное использование информации, систем информационных и технологий в целях усиления средств и сил при осуществлении стратегии операций информационных.

СРЕДСТВА МАССОВОЙ ИНФОРМАЦИИ - 1) периодические печатные издания, радио-, телевидеопрограммы, кинохроникальные программы, иные формы периодического распространения массовой информации [109]; 2) периодические печатные издания, радио-, теле-, видеопрограммы, кинохроникальные программы и иные формы непрерывного или периодического распространения массовой информации. При этом предполагается, что периодическое печатное издание (газета, журнал, альманах, бюллетень) должно иметь постоянное название, текущий номер и выходить в свет не реже одного раза в год.

СРЕДСТВА МЕЖДУНАРОДНОГО ИНФОРМАЦИОННОГО ОБМЕНА - информационные системы, сети и сети связи, используемые при международном информационном обмене.

СРЕДСТВА СВЯЗИ - технические средства, используемые для формирования, обработки, передачи или приема сообщений электросвязи либо почтовых отправлений.

СРЕДСТВА ТЕЛЕКОММУНИКАЦИИ - совокупность средств связи, обеспечивающих передачу данных между ЭВМ и информационными системами, удаленными друг от друга на значительные расстояния.

СРЕДСТВО АКТИВНЫХ ПРЕДНАМЕРЕННЫХ РАДИОЭЛЕКТРОННЫХ ПОМЕХ - средство РЭП, предназначенное для создания активных радио, оптико-электронных, акустических помех.

СРЕДСТВО КОНТРОЛЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ - техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности ЗИ.

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ - средство, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

СРЕДСТВО НЕПОСРЕДСТВЕННОЙ (ИСПОЛНИТЕЛЬНОЙ) РАДИОЭЛЕКТРОННОЙ РАЗВЕДКИ - средство, предназначенное для обнаружения сигналов РЭС противника — объектов (целей) радиоэлектронного подавления и определения их характеристик (параметров),

необходимых для применения средств РЭП.

СРЕДСТВО ПАССИВНЫХ ПРЕДНАМЕРЕННЫХ РАДИОЭЛЕКТРОННЫХ ПОМЕХ - средство РЭП, предназначенное для создания пассивных радио, оптико-электронных, акустических помех.

СРЕДСТВО ПОРАЖЕНИЯ ЭЛЕКТРОМАГНИТНЫМ ИЗЛУЧЕНИЕМ - техническое устройство с мощным электромагнитным излучением, предназначенное для разрушения (повреждения) функциональных узлов (радиоэлектронных элементов) поражаемого РЭС.

СРЕДСТВО РАДИОЭЛЕКТРОННОГО ПОДАВЛЕНИЯ - функционально и конструктивно законченное техническое устройство, предназначенное для создания преднамеренных радио-оптико-электронных или гидроакустических помех.

СРЕДСТВО РАДИОЭЛЕКТРОННОГО ПОРАЖЕНИЯ - общее наименование средств функционального поражения, самонаводящегося на источник радиоизлучения оружия и систем, комплексов, средств РЭП.

СРЕДСТВО РАДИОЭЛЕКТРОННЫХ ПОМЕХ - средство активных преднамеренных радиоэлектронных помех, позволяющее вести непосредственную радиоэлектронную разведку, выбирать объекты РЭП, генерировать с требуемыми для подавления конкретных РЭС структурой и параметрами.

СРЕДСТВО СПЕЦИАЛЬНОГО ПРОГРАММНО-ТЕХНИЧЕСКОГО ВОЗДЕЙСТВИЯ - техническое устройство, предназначенное для внедрения в автоматизированные системы управления противника специальных программам (вирусов), разрушающих программное обеспечение их баз данных (знаний).

СРЕДСТВО ТЕХНИЧЕСКОГО КОНТРОЛЯ - техническое средство, предназначенное для выявления технических каналов утечки информации, демаскирующих признаков в деятельности войск (сил) в ходе боевого применения и использования вооружения, военной техники и военных объектов по одному или нескольким из контролируемых физических полей, а также контролю соблюдения мер по обеспечению электромагнитной совместимости РЭБ в группировках войск (сил).

СРЕДСТВО ФУНКЦИОНАЛЬНОГО ПОРАЖЕНИЯ - общее наименование средств функционального поражения электромагнитным излучением и специального программно-технического воздействия.

СТАНЦИЯ РАДИОЭЛЕКТРОННЫХ ПОМЕХ - средство активных преднамеренных радиоэлектронных помех, позволяющее вести непосредственную радиоэлектронную разведку, выбирать объекты РЭП, генерировать с требуемыми для подавления конкретных РЭС структурой и параметрами.

СТОЙКОСТЬ КРИПТОГРАФИЧЕСКОГО ЗАКРЫТИЯ - минимальная длина закрытого текста, на которой могут быть выявлены такие статистические закономерности, на основе которых может быть восстановлен открытый текст.

СТРАТЕГИЧЕСКОЕ СДЕРЖИВАНИЕ – комплекс согласованных политических, экономических, идеологических, научно-технических, военных и иных мер, проводимых последовательно или одновременно с целью стабилизации военно-политической и военно-стратегической обстановки, сдерживания (локализации) эскалации вооруженного конфликта и предотвращения возможной агрессии.

СТРУКТУРА ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ - организованная соответствующим образом совокупность основных элементов, составляющих единое целое. Структура представлена следующими элементами: субъект, объект, технология воздействия коммуникационный канал, условия воздействия, обратная связь. Наполнена конкретным содержанием, в качестве которого

выступает совокупность видов, форм, методов и приемов психологического воздействия.

СУБЪЕКТ ДОСТУПА (К ИНФОРМАЦИИ) - 1) участник правоотношений в информационных процессах; 2) лицо или процесс, действие которого регламентируется правилами разграничения доступа.

СУБЪЕКТ ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ - элемент структуры психологического воздействия, рассматриваемый как лицо или группа, осуществляющая воздействие, или специальный аппарат, занимающийся проведением психологических операций, со всеми его качественными и количественными характеристиками.

СУБЪЕКТЫ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА - физические и юридические (общественные организации, хозяйствующие субъекты, органы государственной власти) лица, вступающие для реализации своих потребностей или возложенных на них функций во взаимоотношения с использованием информации и инфраструктур информационных. Являются наиболее важной и системообразующей составляющей пространства информационного.

СУБЪЕКТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ - граждане, общественные организации и объединения, обладающие правами и обязанностями по участию в обеспечении безопасности.

СУГГЕСТИВНОЕ ОРУЖИЕ - совокупность способов и средств, предназначенных для подсознательного внушения человеку или группе людей нужного для воздействующей стороны поведения (принимаемых решений, образа мышления, мировоззренческих установок и т.п.). ПО составляет фармакологическую часть психофизического оружия.

ТАЙНА ГОСУДАРСТВЕННАЯ - защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение (утрата) которых может нанести ущерб безопасности Российской Федерации. Необходимость отнесения сведений к государственной тайне определяется министерствами и ведомствами в соответствии с разграничением полномочий между ними и с помощью специальных экспертных комиссий.

ТАЙНА НЕГОСУДАРСТВЕННАЯ - защищаемые в соответствии с законодательством собственником или владельцем информационные ресурсы ограниченного доступа, утрата которых может нанести деловой, экономический, моральный или иной ущерб, потерю престижа юридическим или физическим лицам. К негосударственной тайне относят: служебную, коммерческую (предпринимательскую), личную, семейную тайну, технологические новшества предприятий, профессиональную тайну и др..

ТАЙНА ПРОФЕССИОНАЛЬНАЯ - секретные и конфиденциальные сведения, составляющие государственную или негосударственную тайну юридических и физических лиц, но защищаемые другими полномочными учреждениями, которым эти сведения стали известны в силу их профессиональной деятельности. Профессиональная тайна включает: тайну предприятий связи и транспорта, банковскую, врачебную тайну, тайну налоговых органов, тайну страхования, нотариальную, адвокатскую тайну, тайну органов ЗАГС, тайну исповеди. Одной из главных задач является защита персональных данных граждан, личной и семенной тайны. К профессиональной тайне относят также тайну мастерства.

ТАЙНА СЛУЖЕБНАЯ - конфиденциальные сведения, входящие в понятие информационных ресурсов ограниченного доступа и относящиеся к служебной деятельности государственных учреждений, организаций и предприятий. Доступ к этим сведениям ограничен в интересах обеспечения безопасности информации указанных структур. Подобные сведения не подлежат широкому распространению, оглашению или опубликованию в средствах массовой информации и используются исключительно в целях решения управленческих или производственных задач, например, проекты готовящихся документов, рабочие инструкции и др. Состав сведений, составляющих служебную тайну, определяется руководством учреждений, организаций и предприятий. Отнесением к служебной тайне защищаются персональные данные, концентрируемые в

службах персонала (отделах кадров) государственных и негосударственных структур. К служебной информации ограниченного распространения не могут быть отнесены: законодательные акты, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации; сведения о чрезвычайных ситуациях; описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также адрес; порядок рассмотрения и разрешения заявлений и обращений граждан и юридических лиц; сведения об исполнении бюджета; документы, накапливаемые в открытых фондах библиотек и архивов.

ТЕРРОРИЗМ - совершение взрыва, поджога или иных действий, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, если эти действия совершены в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти, а также угроза совершения указанных действий в тех же целях.

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ - защита (не криптографическими методами) информации от ее утечки по техническим каналам, от несанкционированного доступа или от специальных воздействий на информацию в целях ее уничтожения, искажения и блокирования, и противодействие ТСР.

ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ - мероприятия по ЗИ, предусматривающие применение технических средств и решений по предотвращению утечки защищаемой информации от иностранной технической разведки.

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ - аппаратные (встроенные в аппаратуру) и функционирующие автономно (независимо от аппаратуры) технические средства, обеспечивающие техническую защиту конфиденциальной информации.

ТЕХНИЧЕСКИЙ АНАЛИЗ РАДИОСИГНАЛОВ - процесс радиоразведки, целью которого является определение технических параметров радиосигналов (частотных, фазовых, временных, амплитудных).

ТЕХНИЧЕСКИЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ - физический путь от источника конфиденциальной информации к нарушителю ИБ, по которому возможно несанкционированное получение охраняемых сведений (совокупность источника конфиденциальной информации, физической среды и нарушителя ИБ).

ТЕХНИЧЕСКИЙ КОНТРОЛЬ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ - контроль эффективности защиты информации, проводимый с использованием технических средств контроля.

ТЕХНОЛОГИЯ ВОЗДЕЙСТВИЯ - согласованный процесс применения информационных способов и средств. В информационной борьбе рассматривается как стратегия и тактика их применения.

ТОЧНОСТЬ ИНФОРМАЦИИ - термин используется для характеристики того, что информация поддержана и передана таким способом, что не могла измениться ни злонамеренно, ни случайно. Точность гарантирует против подделки или вмешательства. Нередко трактуется как синоним целостности.

ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ - руководящие документы, регламентирующие качественные и количественные критерии безопасности информации и нормы эффективности ее защиты.

УБЕЖДЕНИЕ - метод информационно-психологического воздействия в психологической операции, рассматриваемый как плановое, целенаправленное воздействие на объект (группу объектов), апеллирующее к рациональной сфере его сознания в целях формирования, закрепления или изменения установок, изменения поведения объекта в соответствии с целями психологической

операции.

УГОЛКОВЫЙ ОТРАЖАТЕЛЬ - средство пассивных радиоэлектронных помех, представляющее собой конструкцию, образованную тремя взаимно перпендикулярными зеркально отражающими плоскостями.

УГРОЗА - совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности.

УГРОЗА БЕЗОПАСНОСТИ ИНФОРМАЦИИ - 1) совокупность условий и факторов, создающих потенциальную или реальную опасность, связанную с утечкой информации и/или несанкционированными, и/или непреднамеренными воздействиями на нее; 2) фактор или совокупность факторов, создающих опасность функционированию, сохранению и развитию информационного пространства.
Основными угрозами безопасности телекоммуникационных средств и систем могут являться:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и телекоммуникационных систем, в том числе систем ЗИ;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической ЗИ;
- утечка информации по техническим каналам;
- внедрение радиоэлектронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование не сертифицированных отечественных и зарубежных информационных технологий, средств ЗИ, средств информатизации, телекоммуникации и связи;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

УГРОЗА ПАССИВНАЯ - угроза неправомочного раскрытия информации без того, чтобы изменять состояние системы. Тип угрозы, которая подразумевает только перехват, но не изменение или уничтожение информации.

УГРОЗА СИСТЕМЕ ПЕРЕДАЧИ ДАННЫХ - реализованная опасность СПД, состоящая в разрушении информации или других ресурсов; искажении или модификацию информации; хищении, удалении или потере информации и/или других ресурсов; раскрытии информации; прерывании обслуживания.

УГРОЗЫ БЕЗОПАСНОСТИ - совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ - подразделяют на случайные и преднамеренные, активные и пассивные.
К основным видам угроз ИБ РФ можно отнести следующие:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному

сознанию, духовному возрождению России;

- угрозы информационному обеспечению государственной политики РФ;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозы информационной безопасности в общегосударственных информационных и телекоммуникационных системах:

- деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных и телекоммуникационных систем;
- вынужденное в силу объективного отставания отечественной промышленности использование при создании и развитии информационных и телекоммуникационных систем импортных программно-аппаратных средств;
- нарушение установленного регламента сбора, обработки и передачи информации, преднамеренные действия и ошибки персонала информационных и телекоммуникационных систем, отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;
- использование не сертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты информации и контроля их эффективности;
- привлечение к работам по созданию, развитию и защите информационных и телекоммуникационных систем организаций и фирм, не имеющих государственных лицензий на осуществление этих видов деятельности.

Угрозы информационной безопасности в сфере внешней политики:

внешние угрозы:

- информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики РФ;
- распространение за рубежом дезинформации о внешней политике РФ;
- нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;
- попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику РФ, российских представительств и организаций за рубежом и при международных организациях;

внутренние угрозы:

- нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти, реализующих внешнюю политику РФ, и на подведомственных им предприятиях, в учреждениях и организациях;
- информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности РФ;
- недостаточная информированность населения о внешнеполитической деятельности Российской Федерации.

Угрозы информационной безопасности в сфере обороны:

- все виды разведывательной деятельности зарубежных государств;
- информационно-технические воздействия (в том числе РЭБ, проникновение в компьютерные сети) со стороны вероятных противников;
- диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия;
- деятельность иностранных политических, экономических и военных структур, направленная против интересов РФ в сфере обороны;

внутренними угрозами, представляющими наибольшую опасность в сфере обороны, являются:

– нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в штабах и учреждениях МО РФ, на предприятиях оборонного комплекса;
– преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем специального назначения;
– ненадежное функционирование информационных и телекоммуникационных систем специального назначения;
– возможная информационно-пропагандистская деятельность, подрывающая престиж ВС РФ и их боеготовность;
– нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов;
– нерешенность вопросов социальной защиты военнослужащих и членов их семей.

Угрозы информационной безопасности в условиях чрезвычайных ситуаций, сокрытие, задержка поступления, искажение и разрушение оперативной информации, несанкционированный доступ к ней отдельных лиц или групп лиц могут привести как к человеческим жертвам, так и к возникновению сложностей при ликвидации ЧС, связанных с особенностями информационного воздействия в экстремальных условиях: к приведению в движение больших масс людей, испытывающих психический стресс; к быстрому возникновению и распространению среди них паники и беспорядков на основе слухов, ложной или недостоверной информации.

Угрозы национальной безопасности России в информационной сфере:

– стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка;
– разработка рядом государств концепции информационных войн, нарушение нормального функционирования информационных и телекоммуникационных систем; сохранности информационных ресурсов, получения несанкционированного доступа к ним.

УГРОЗЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ В ИНФОРМАЦИОННОЙ СФЕРЕ - стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним.

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ - система регулярных защитных мероприятий, направленных на обеспечение безопасности в соответствии с изменяющимися условиями внутренней и внешней среды.

УПРАВЛЕНИЕ ВОСПРИЯТИЕМ - в данном контексте следует относить к методам воздействия информационно-психологического. Действия, сводящиеся к передаче или селектированию информации и индикаторов восприятия и имеющие целью влиять на эмоции, поводы и объективное рассуждение субъектов восприятия. Нацелено, в первую очередь, на интеллектуальную элиту общества страны противника и лидеров всех уровней с тем чтобы влиять на официальные оценки, в конечном счете заканчивающиеся официальными действиями, благоприятными целям субъекта восприятием управления. Различными способами восприятием управление комбинирует проектирование правды, безопасность действий, сокрытие и обман, а также специальные психологические действия.

УПРАВЛЕНИЕ ДОСТУПОМ - способ защиты информации путем регулирования использования ресурсов (документов, технических и программных средств, элементов баз данных и т.п.). Управление доступом включает следующие функции защиты: идентификацию пользователей, персонала и ресурсов; проверку полномочий, разрешение и создание условий работы в пределах установленного регламента; регистрацию (протоколирование) обращения к защищаемой информации; реагирование при попытках несанкционированного действия.

УСЛОВИЯ ВОЗДЕЙСТВИЯ - элемент структуры психологического воздействия, рассматриваемый как коммуникативная ситуация, в рамках которой осуществляется психологическое воздействие.

УСТОЙЧИВОСТЬ СИСТЕМЫ ВОЕННОЙ СВЯЗИ - способность СВС обеспечивать управление войсками (силами) и оружием в условиях вредных воздействий.

УТЕЧКА ИНФОРМАЦИИ - 1) неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками; 2) неконтролируемый выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация доверена.

УЯЗВИМОСТИ АНАЛИЗ - в операциях информационных — систематические проверки системы информационной или ее продукции для определения адекватности мер обеспечения безопасности, выяснения дефектов системы мер безопасности, получения данных, позволяющих предсказать эффективность предполагаемых мер безопасности и подтвердить адекватность таких мер после выполнения.

УЯЗВИМОСТЬ ИНФОРМАЦИИ - объективное свойство информации подвергать различного рода воздействиям (опасностям, угрозам), нарушающим ее целостность, достоверность и *конфиденциальность*. Воздействия носят дестабилизирующий по отношению к информации характер и приводят *к утрате носителя конфиденциальной информации или утрате конфиденциальности информации*. Уровень уязвимости информации находится в прямой зависимости с степени совершенства применяемой в фирме *системы защиты информации*, перекрытия этой системой всей сферы *возможных угроз* и предполагаемых *каналов несанкционированного доступа к информации*.

ФАКТОР, ВОЗДЕЙСТВУЮЩИЙ НА ЗАЩИЩАЕМУЮ ИНФОРМАЦИЮ - явление, действие или процесс, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации и блокирование доступа к ней.

ФИЗИЧЕСКАЯ ЗАЩИТА - средства, используемые для физической защиты ресурсов от преднамеренной или случайной угрозы.

ФИЗИЧЕСКАЯ ОХРАНА СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ - система мер, предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время.

ФИЗИЧЕСКОЕ ВОЗДЕЙСТВИЕ - согласованное применение огневых (ядерных) средств, а также подразделений специального назначения для уничтожения (поражения, вывода из строя, захвата) критически важных информационных объектов противника в целях наращивания усилий информационного воздействия и защиты, как в ходе огневого поражения противника, так и по планам информационных операций (действий, акций).

ФОРМЫ ВЕДЕНИЯ ИНФОРМАЦИОННОЙ БОРЬБЫ — информационное воздействие, информационная атака, информационное сражение и информационная операция.

Информационное воздействие, организованное применение сил и средств ИБ для решения задач по завоеванию (поддержанию) информационного превосходства над противником.

Информационная атака, совокупность активных информационных воздействий сил и средств отдельных подразделений на элемент или группу элементов информационных систем противника в целях решения частных тактических задач ИБ.

Информационное сражение, совокупность различных информационных воздействий и атак, объединенных общим замыслом, проводимых специально выделенными силами и средствами и направленных на решение одной оперативной задачи ИБ.

Информационная операция, совокупность согласованных по цели, задачам, месту и времени информационных воздействий, атак и сражений, проводимых по единому замыслу и плану для решения задач ИБ на театре военных действий, стратегическом или операционном направлении.

ФУНКЦИОНАЛЬНОЕ ПОРАЖЕНИЕ - радиоэлектронное поражение, заключающееся в разрушении (повреждении) элементов и узлов радиоэлектронных объектов, информации

противника. Ф.п. включает: поражение электромагнитным излучением и средствами специального программно-технического воздействия.

ФУНКЦИОНАЛЬНЫЙ ОБЪЕКТ - элемент программы, осуществляющий выполнение действий по реализации законченного фрагмента алгоритма программы.

ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ - 1) способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения); 2) состояние информации и ее носителей, при котором обеспечивается неизменность формы представления и содержания информации при несанкционированном и/или непреднамеренном воздействии на информацию и/или ее носитель; 3) актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения; 4) неизменность и неразделимость информации при ее хранении и передаче внутри системы или сети.

ЦЕЛЬ ЗАЩИТЫ ИНФОРМАЦИИ - заранее намеченный результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и(или) несанкционированного и непреднамеренного воздействия на информацию.

ЦЕНЗУРА МАССОВОЙ ИНФОРМАЦИИ - требование от редакции средства массовой информации со стороны должностных лиц, государственных органов, организаций, учреждений или общественных объединений предварительно согласовывать сообщения и материалы (кроме случаев, когда должностное лицо является автором или интервьюируемым), а равно наложение запрета на распространение сообщений и материалов, их отдельных частей.

ШИФР - 1) совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей; 2) совокупность условных знаков, используемых для преобразования открытой информации в вид, исключающий ее восстановление (дешифрование), если наблюдающий (перехватывающий) не имеет сведений (ключа) для раскрытия шифра.

ШИФРОВАЛЬНЫЕ СРЕДСТВА (средства криптографической защиты информации) - 1) реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для ЗИ (в том числе и входящие в системы и комплексы ЗИ от несанкционированного доступа), циркулирующей в технических средствах, при ее обработке, хранении и передаче по каналам связи, включая шифровальную технику; 2) реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и электронной цифровой подписи; в) аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для изготовления и распределения ключевых документов, используемых в шифровальных средствах, независимо от вида носителя ключевой информации; г) ручные шифры, документы кодирования и другие носители ключевой информации; 3) средства, осуществляющие криптографические преобразования информации для обеспечения ее безопасности.

ШИФРОВАНИЕ - 1) процесс зашифрования или расшифрования; 2) криптографическое преобразование данных для получения шифротекста. Шифрование может быть необратимым процессом, в связи с чем соответствующий процесс дешифрования невозможно реализовать; 3) математическое, алгоритмическое (криптографическое) преобразование данных с целью получения шифрованного текста. Шифрование может быть предварительное (шифруется текст документа) и линейное (шифруется разговор). Кроме того, бывает шифрование блочное (каждый очередной блок шифруется независимо) и поточное (каждый знак шифруется независимо от других).

ШИФРОТЕКСТ - данные, получаемые в результате использования шифрования.

ЭКРАНИРОВАНИЕ - функция межсетевого экрана, позволяющая поддерживать безопасность объектов внутренней области, игнорируя несанкционированные запросы из внешней области.

ЭКРАНИРУЮЩЕЕ СООРУЖЕНИЕ ОБЪЕКТА ЗАЩИТЫ - специальное производственное сооружение, предназначенное для отработки объекта защиты или его систем и обеспечивающее его защиту от средств разведки за счет поглощающих свойств конструкции указанного сооружения.

ЭЛЕКТРИЧЕСКАЯ СВЯЗЬ (ЭЛЕКТРОСВЯЗЬ) - всякая передача или прием знаков, сигналов, письменного текста, изображений, звуков по проводной, радио-, оптической и другим электромагнитным системам.

ЭЛЕКТРОАКУСТИЧЕСКИЙ КАНАЛ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ - канал утечки речевой информации, обусловленный преобразованием акустических колебаний в электрические и обратно и распространением этих колебаний в различных присущих им средах.

ЭЛЕКТРОМАГНИТНАЯ ДОСТУПНОСТЬ - максимальная дальность до разведываемого радиоэлектронного объекта, при которой обеспечивается надежный радиоконтакт его со средствами РР (НРТР).

ЭЛЕКТРОМАГНИТНОЕ ПОДАВЛЕНИЕ - преднамеренное подавляющее или маскирующее воздействие электромагнитной энергией на РЭС. Электромагнитное подавление, осуществляемое в радиодиапазоне, целесообразно именовать радиоподавлением, в диапазоне световых (оптических) волн – световым подавлением.

ЭЛЕКТРОМАГНИТНЫЕ НАВОДКИ - токи и напряжения в токопроводящих элементах, электрические заряды или магнитные потоки, вызванные электромагнитным полем.

ЭЛЕКТРОМАГНИТНЫЕ ПОМЕХИ - 1) наличие нежелательного электромагнитного излучения, которое может привести к повреждению данных; 2) непоражающие электромагнитные излучения, которые ухудшают качество функционирования РЭС, работающих на принципе приема, усиления и преобразования электромагнитных сигналов. Создаваемые в диапазоне радиоволн электромагнитные помехи именуют радиопомехами, в световом (оптическом) диапазоне – световыми.

ЭЛЕКТРОМАГНИТНЫЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ - физический путь от источника побочных электромагнитных излучений и наводок (ПЭМИН) различных технических средств к злоумышленнику за счет распространения электромагнитной энергии в воздушном пространстве и направляющих системах.

ЭЛЕКТРОННОЕ СООБЩЕНИЕ - информация, представленная в форме набора состояний элементов электронной вычислительной техники, иных электронных средств обработки, хранения и передачи информации, могущей быть преобразованной в форму, пригодную для однозначного восприятия человеком.

ЭФФЕКТИВНОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ - 1) степень соответствия результатов защиты информации поставленной цели; 2) степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Конституция Российской Федерации от 12 декабря 1993 г. - М.: 1993.
2. Гражданский кодекс Российской Федерации. Федеральный закон от 17 декабря 1999 г. № 213.
3. Уголовный кодекс Российской Федерации. Федеральный закон от 9 июля 1999 г. № 157.
4. Налоговый кодекс Российской Федерации. Федеральный закон от 5 августа 2000 г. № 118.
5. О безопасности. Закон Российской Федерации от 5 марта 1992 г. № 2446-1.
6. О государственной тайне. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 с изменениями и дополнениями, внесенными 6 октября 1997 г. № 131-ФЗ.
7. Об информации, информатизации и защите информации. Федеральный закон от 20 февраля 1995 г. № 24.
8. Об участии в международном информационном обмене. Федеральный закон от 4 июля 1996 г. № 85.
9. О связи. Федеральный закон от 16 февраля 1995 г. № 15.
10. О сертификации продукции и услуг. Закон Российской Федерации от 10 июня 1993 г. № 5151-1.
11. О стандартизации. Закон Российской Федерации от 10 июня 1993 г. № 5451.
12. О лицензировании отдельных видов деятельности. Федеральный закон от 25 сентября 1998 г. № 158.
13. О внешней разведке. Федеральный закон от 10.01.96 N 5-ФЗ.
14. О защите прав потребителей. Закон Российской Федерации от 07 февраля 1992 г. № 2300.
15. О внешней разведке. Федеральный закон от 10 января 1996 г. № 5.
16. Об органах Федеральной службы безопасности в Российской Федерации. Федеральный закон от 3 апреля 1995 г. № 40.
17. Об оперативно-розыскной деятельности. Федеральный закон от 12 августа 1995 г. № 144.
18. О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера. Федеральный закон от 21 декабря 1994 г. № 68.
19. О федеральных органах правительственной связи и информации. Закон Российской Федерации от 19 февраля 1993 г. № 4524-1 с изменениями по Указу Президента Российской Федерации от 24 декабря 1993 г. № 2288.
20. Об авторском праве и смежных правах. Закон Российской Федерации от 9 июля 1993 г. № 5351-1 с изменениями от 19 июля 1995 г.
21. О правовой охране программ для электронных вычислительных машин и баз данных. Закон Российской Федерации от 23 сентября 1992 г. № 3523-1.
22. О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации. Федеральный закон от 13.01.95 N 7-ФЗ.
23. О военно-техническом сотрудничестве Российской Федерации с иностранными государствами. Федеральный закон от 19 июля 1998 г. № 114.
24. Об электронной цифровой подписи. Проект Федерального закона.
25. Об охране здоровья граждан. Постановление Верховного Совета Российской Федерации от 22 июля 1993 г. № 5487.
26. О средствах массовой информации. Закон Российской федерации от 27.12.91 N 2124-I.

27. Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации. Федеральный закон от 19.09.97 N 124-ФЗ.

28. О государственной поддержке средств массовой информации и книгоиздания Российской Федерации. Федеральный закон от 01.12.95 N 191-ФЗ.

29. Концепция национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 10 января 2000 г. № 24.

30. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 09 сентября 2000 г. Пр-1895.

31. Положение о Министерстве внутренних дел Российской Федерации. Указ Президента Российской Федерации от 18 июля 1996 г. №1039.

32. Положение о Государственной технической комиссии при Президенте Российской Федерации. Указ Президента Российской Федерации от 19 февраля 1999 г. № 212.

33. Перечень сведений, отнесенных к государственной тайне: Указ Президента Российской Федерации от 24 января 1998 г. № 61.

34. Положение о Межведомственной комиссии по защите государственной тайны. Указ Президента Российской Федерации от 20 января 1996 г. № 71.

35. Перечень сведений конфиденциального характера. Указ Президента Российской Федерации от 6 марта 1997 г. № 188.

36. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности. Постановление Правительства Российской Федерации от 4 сентября 1995 г. № 870.

37. Положение о лицензировании отдельных видов деятельности. Постановление Правительства Российской Федерации от 11 апреля 2000 г. № 326.

38. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233.

39. Положение о порядке разработки, производства, реализации и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (ПКЗ-99).

40. Национальная технологическая база (1996-2005 гг.): Программа. Постановление Правительственной комиссии по научно-технической политике от 21 июля 1996 г. 2727п-П.

41. Временное положение о государственном учете и регистрации баз и банков данных", утвержденное постановлением Правительства Российской Федерации от 28.02.96 N 226, п. 3.

42. Положение о системе сертификации ГОСТ Р. Постановление Государственного комитета Российской Федерации от 17 марта 1998 г. № 11.

43. Положение о сертификации средств защиты информации. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608, от 29 марта 1999 г. № 509.

44. Положение о сертификации средств защиты информации по требованиям безопасности информации. Приказ Гостехкомиссии России от 27 октября 1995 г. № 199.

45. Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и/или оказанием услуг по защите государственной тайны. Постановление Правительства Российской Федерации от 15 апреля 1995 г. № 333.

46. Положение о государственном лицензировании деятельности в области защиты информации. Решение Гостехкомиссии России и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27 апреля 1994 г. № 10 и от 24 июня 1997 г. № 60.

47. Положение по аттестации объектов информатизации по требованиям безопасности информации: Утверждено Председателем Гостехкомиссии России 25 ноября 1994 г.

48. О порядке проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну: Инструкция. Утверждена Директором Федеральной службы безопасности Российской Федерации 23 августа 1995 г. № 28.

49. О порядке проведения специальных экспертиз предприятий, учреждений и организаций на право осуществления мероприятий и (или) оказания услуг в области противодействия иностранной технической разведке: Инструкция. Утверждена Председателем Государственной технической комиссии при Президенте Российской Федерации 17 октября 1995 г.

50. Государственная система стандартизации Российской Федерации. Основные положения. ГОСТ Р 1.0-92.

51. Системы обработки информации. Термины и определения. ГОСТ Р 15971-90.

52. Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения. ГОСТ 16504-81.

53. Внешние воздействующие факторы. Термины и определения. ГОСТ 26883-86.

54. Защита криптографическая. Алгоритм криптографического преобразования. ГОСТ 28147-89.

55. Автоматизированные системы. Термины и определения. ГОСТ 34.003-90.

56. Защита от несанкционированного доступа к информации. Общие требования к органам по сертификации продукции и услуг. ГОСТ Р 50739-95.

57. Защита информации. Основные термины и определения. ГОСТ Р 50922-96.

58. Научные основы энергоинформационных взаимодействий в природе и обществе: Материалы международного конгресса «ИнтерЭНИО-97». –М.: МАЭН, 1997. — 268 с.

59. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. ГОСТ Р 51188-98.

60. Автоматизированные системы в защищенном исполнении. Общие требования. ГОСТ Р 51624-00.

61. Факторы, воздействующие на информацию. Общие положения. ГОСТ Р 51275-99.

62. Военная техника. Термины и определения. ГОСТ РВ 51540-99.

63. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. ГОСТ 51583-00.

64. Государственный комитет Российской Федерации по стандартизации, метрологии и сертификации. Основные положения. Система сертификации ГОСТ.

65. Архитектура защиты информации. ГОСТ Р ИСО 7498-2-99.

66. Надежность и качество услуг. Международный стандарт CEI IEC 50 (191).

67. Защита информации об авиационной технике и вооружении от иностранных технических разведок. Термины и определения. ОСТ В1 00464-97.

68. Система обеспечения информационной безопасности Взаимоувязанной сети связи Российской Федерации. Термины и определения. ОСТ 45.127-99.

69. Защита от несанкционированного доступа к информации. Термины и определения: Сборник руководящих документов по защите информации от несанкционированного доступа. -М.: Гостехкомиссия России, 1998.

70. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации: Сборник руководящих документов по защите информации от несанкционированного доступа. -М.: Гостехкомиссия России, 1998.

71. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации: Руководящий документ // Сборник руководящих документов по защите информации от несанкционированного доступа. - М.: Гостехкомиссия России, 1998.

72. Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам. Постановление Совета Министров Правительства Российской Федерации от 15 сентября 1993 г. № 912-51.

73. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники: Сборник руководящих документов по защите информации от несанкционированного доступа. -М.: Гостехкомиссия России, 1998.

74. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации: Сборник руководящих документов по защите информации от несанкционированного доступа. -М.: Гостехкомиссия России, 1998.

75. Специальные защитные знаки. Классификация и общие требования. // Сборник руководящих документов по защите информации от несанкционированного доступа. -М.: Гостехкомиссия России, 1998.

76. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации. // Сборник руководящих документов по защите информации от несанкционированного доступа. -М.: Гостехкомиссия России, 1998.

77. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей: Приказ Председателя Гостехкомиссии России от 4 июня 1999 г. № 114.

78. Терминология в области защиты информации. Справочник. ВНИИстандарт. 1993.

79. Прокофьев В.Ф. Тайное оружие информационной войны – М.: СИНТЕГ, 1999. — 152 с.

80. Емельянов Г.В., Стрельцов А.А. Информационная безопасность России. Часть 1. Основные понятия и определения: Уч. пос. / Под общ. ред. А.А. Прохожева. –М.: РАГС при Президенте Российской Федерации, 1999. — 52 с.

81. Приходько А.Я. Словарь-справочник по информационной безопасности. –М.: СИНТЕГ, 2001. — 124 с.

82. Ярочкин В.И., Шевцова Т.А. Словарь терминов и определений по безопасности и защите информации. –М.: «Ось-89», 1996. — 48 с.

83. Доктрина совместных действий по проведению информационных операций. Наставление объединенного штаба Комитета начальников штабов ВС США 3-13. / Пер. с англ. –М.: МО РФ, 1999. — 50 с.

84. Концепция информационной войны США: Информация. –М.: МО РФ, 1994. — 44 с.

85. Информационные вызовы национальной и международной безопасности / Под. общ. ред. А.В. Федорова, В.Н. Цыгичко. –М.: ПИР-Центр, 2001. — 328 с.

86. Синклер А. Большой толковый словарь компьютерных терминов. Русско-английский, англо-русский. –М.: Вече, АСТ, 1998. — 512 с.

87. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Уч. пос. –М.: ИНФРА-М, 2001. — 304 с.

88. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных: Уч. пос. –М.: СИНТЕГ, 2002. — 248 с.

89. Палий А.И. Радиоэлектронная борьба. 2-е изд., перераб. и доп. –М.: Воениздат, 1989. — 350 с.

90. Анализ работ, проводимых за рубежом в интересах создания оружия нелетального действия: Рабочие материалы. – М.: МО РФ, 1995. — 56 с.

91. Поздняков А.И. Информационная безопасность страны и вооруженных сил /Актуальные проблемы национальной безопасности. –М.: ВАГШ, 2000.

92. Положение о государственной системе защиты информации в Российской Федерации. –М.: Гостехкомиссия России, 1993. — 12 с.

93. Хорев А.А. Способы и средства защиты информации. –М.: Минобороны, 2000. — 320 с.

94. Коротченко Е.Г. Информационно-психологическое противоборство в современных условиях. –М.: Военная мысль, 1996, № 1. С. 22-28.

95. Мельников В.В. Защита информации в компьютерных системах. –М.: Финансы и статистика; Электроинформ, 1997. — 368 с.

96. Емельянов Г.В., Стрельцов А. А.. Информационная безопасность (учебное пособие). - М. 1999.

97. Некоторые вопросы предотвращения утечки информации. Борьба с промышленным шпионажем. –М.: ОАО «НОВО», 2001. — 50 с.

98. Современные технологии безопасности. Каталог-2002. –М.: МАСКОМ, Центр безопасности информации, 2002. — 52 с.

99. Гражданская защита. Понятийно-терминологический словарь / Под общ. ред. Ю.Л. Воробьева. – М.: Изд. «Флайст», Инф. изд. центр «Геополитика», 2001. — 240 с.

100. Патентный закон Российской Федерации. Закон Российской Федерации от 23 сентября 1992 г., № 3517-1.

101. Об архивном фонде Российской Федерации и архивах. Закон Российской Федерации от 7 июля 1993 г., № 5341-1.

102. О государственной поддержке средств массовой информации и книгоиздания Российской Федерации. Федеральный закон от 1 декабря 1995 г. № 191-ФЗ.

103. Терминология в области защиты информации: Справочник ВНИИстандарт, 1993.

104. О передаче предоставления Российской Федерацией военного и гражданского персонала для участия в деятельности по поддержанию или восстановлению международного мира и безопасности. Федеральный закон от 23 июня 1995 г. № 93-ФЗ.

105. О федеральных органах правительственной связи и информации. Закон Российской Федерации от 19 февраля 1993 г. № 4524-1.

106. О государственной охране. Федеральный закон от 13 октября 1995 г. № 157-ФЗ.

107. Комов С.А. О способах и формах ведения информационной борьбы // «Военная мысль», 1997, № 4. С. 18-22.

108. О рекламе. Федеральный закон от 18 июля 1995 г. № 108-ФЗ.

109. О средствах массовой информации. Закон Российской Федерации от 27 декабря 1991 г. № 2124-1.

110. Концепция защиты информации в системах ее обработки. –М.: Гостехкомиссия России, 1995.

111. Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения. ГОСТ 34.003-90.

112. Родионов М.А. О терминологии теории информационной борьбы / «Проблемы военной науки», 1997, № 6.

113. Связь военная. Термины и определения. ГОСТ В. 23609-86.

114. Совместимость радиоэлектронных средств электромагнитная. Термины и определения. ГОСТ 23611-79.

115. Совместимость технических средств электромагнитная. Термины и определения. ГОСТ Р 50397-92.

116. Положение о Федеральном агентстве правительственной связи и информации при Президенте Российской Федерации. Указ Президента Российской Федерации от 3 апреля 1995 г. № 334.

117. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ-Санкт-Петербург, 2000. Приложение. Англо-русский криптографический словарь с толкованиями.

118. Палий А.И. Проблемы обеспечения информационной безопасности России / Информационный сборник ЦСИ ГЗ МЧС России, 2002, № 8.

119. Палий А.И. Методология общей классификации средств и способов поражения и защиты в природе и обществе. / «Безопасность», 1994, № 7 – 12(23). С. 31-42.

120. Ярочкин В.И. Информационная безопасность. –М.: Международные отношения, «Летописец», 2000.