МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Кафедра информационной безопасности

Составители
Е. В. Прокопенко
И. В. Чичерин

БЕЗОПАСНОСТИ СЕТЕЙ ЭЛЕКТРОННЫХ ВЫЧИСЛИТЕЛЬНЫХ МАШИН

Методические материалы

Рекомендованы учебно-методической комиссией специальности 10.05.03 Информационная безопасность автоматизированных систем в качестве электронного издания для использования в образовательном процессе

Кемерово 2018

Рецензенты

Стенин Д. В.– кандидат технических наук, доцент директор ИИТМА
Сыркин И. С. – кандидат технических наук, доцент кафедры информационных и автоматизированных производственных систем

Прокопенко Евгения Викторовна
Чичерин Иван Владимирович

Безопасности сетей электронных вычислительных машин: методические материалы [Электронный ресурс] для обучающихся специальности 10.05.03 Информационная безопасность автоматизированных систем очной формы обучения / сост. Е. В. Прокопенко, И. В. Чичерин; КузГТУ. – Электрон. издан. – Кемерово, 2018.

1. Основные понятия информационных сетей
2. Основы построения современных локальных сетей

Информационная сеть – *information network* – это сложная распределенная в пространстве система, состоящая из множества сосредоточенных подсистем (узлов), располагающих программно-аппаратными средствами реализации тех или иных составляющих информационных процессов, и множества средств, обеспечивающих соединение и взаимодействие этих подсистем с целью предоставления территориально удаленным пользователям (абонентам) широкого набора услуг из сферы информационного обслуживания.

Абонент – *subscriber* – устройство, юридическое лицо, физическое лицо, имеющее право на взаимодействие с информационным объектом, предоставляющим услуги – системой, сетью, комплексом.

Узел – *node* – компьютер, терминал или любое другое устройство, подключенное к сети. Каждому узлу сети присвоен уникальный адрес, позволяющий другим компьютерам сети связываться с ним.

Хост – *host* – установленный в узлах сети компьютер (сервер), решающий вопросы коммуникации и доступа к сетевым ресурсам.

Сервер – *server* – компьютер, подключенный к сети, или выполняющаяся на нем программа, предоставляющие клиентам доступ к общим ресурсам и управляющие этими ресурсами.

Сервис – *service* – совокупность средств для обслуживания пользователей; набор функций одного из уровней программной структуры сети, обеспечивающих доступ к объектам вышележащего уровня через интерфейс между этими уровнями.

Адрес – *address* – закодированное обозначение пункта отправления либо назначения данных; идентификация объекта сети.

Порт – *port* – точка доступа к устройству либо программе.

В сетях с небольшим количеством компьютеров (10–30) чаще всего используется одна из типовых топологий – общая шина, кольцо или звезда. Все перечисленные топологии обладают свойством однородности, то есть все компьютеры в такой сети имеют одинаковые права в отношении доступа к другим компьютерам (за исключением центрального компьютера при соединении звезда). Такая однородность структуры делает простой процедуру наращивания числа компьютеров, облегчает обслуживание и эксплуатацию сети.

Однако в больших сетях использование типовых структур порождает различные ограничения, важнейшими из которых являются:

– ограничения на длину связи между узлами;

– ограничения на количество узлов в сети;

– ограничения на интенсивность трафика, порождаемого узлами сети.

Например, технология Ethernet на тонком коаксиальном кабеле позволяет использовать кабель длиной не более 185 метров, к которому можно подключить не более 30 компьютеров. Однако, если компьютеры интенсивно обмениваются информацией между собой, иногда приходится снижать число подключенных к

кабелю компьютеров до 20, а то и до 10, чтобы каждому компьютеру доставалась приемлемая доля общей пропускной способности сети.

Для снятия этих ограничений используются специальные методы структуризации сети и специальное структурообразующее оборудование – повторители, концентраторы, мосты, коммутаторы, маршрутизаторы. Оборудование такого рода также называют коммуникационным.

Физическая структуризация – это конфигурация связей, образованных отдельными частями кабеля.

Для физической структуризации применяют следующие устройства.

1. **Повторитель** – *repeater* – простейшее из коммуникационных устройств, используется для физического соединения различных сегментов кабеля локальной сети с целью увеличения общей длины сети. Повторитель передает сигналы, приходящие из одного сегмента сети, в другие ее сегменты. Повторитель позволяет преодолеть ограничения на длину линий связи за счет улучшения качества передаваемого сигнала – восстановления его мощности и амплитуды, улучшения фронтов и т.п.

2. **Концентраторы** характерны практически для всех базовых технологий локальных сетей: Ethernet, ArcNet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet, l00VG-AnyLAN.

Концентраторы повторяют сигналы, пришедшие с одного из своих портов, на других своих портах. Разница между концентраторами разных технологий состоит в том, на каких именно портах повторяются входные сигналы. Концентратор всегда изменяет физическую топологию сети, но при этом оставляет без изменения ее логическую топологию.

Физическая структуризация сети с помощью концентраторов полезна не только для увеличения расстояния между узлами сети, но и для повышения ее надежности.

Любая сеть имеет основные структурные компоненты: внутренние и внешние узлы (оконечные пункты), каналы и линии связи. Узлы связаны между собой каналами передачи данных и образуют в совокупности одну из важных составных частей ИС – сеть передачи данных. Каждый из узлов через блок сопряжения соединен с одним из оконечных абонентских пунктов, в которых размещаются средства информационной и вычислительной техники. По назначению и составу технических средств оконечные пункты сильно различаются друг от друга.

Физическая структуризация сети полезна во многих отношениях, однако в ряде случаев, обычно относящихся к сетям большого и среднего размера, невозможно обойтись без логической структуризации сети.

Логическая структуризация сети – это процесс разбиения сети на сегменты с локализованным трафиком (локализация трафика – распространение трафика, предназначенного для компьютеров некоторого сегмента сети, только в пределах этого сегмента).

Для логической структуризации сети используются такие коммуникационные устройства, как мосты, коммутаторы, маршрутизаторы и шлюзы.

1. **Мост** – *bridge* – делит разделяемую среду передачи сети на части (часто называемые логическими сегментами), передавая информацию из одного сегмента в другой только в том случае, если такая передача действительно необходима, то есть если адрес компьютера назначения принадлежит другой подсети. Тем самым мост изолирует трафик одной подсети от трафика другой, повышая общую производительность передачи данных в сети. Локализация трафика не только экономит пропускную способность, но и уменьшает возможность несанкционированного доступа к данным, так как кадры не выходят за пределы своего сегмента и их сложнее перехватить злоумышленнику.

Применение мостов приводит к значительным ограничениям на конфигурацию связей сети – сегменты должны быть соединены таким образом, чтобы в сети не образовывались замкнутые контуры.

2. **Коммутатор** – *switch, switching hub* – по принципу обработки кадров ничем не отличается от моста. Основное его отличие от моста состоит в том, что он является своего рода коммуникационным мультипроцессором, так как каждый его порт оснащен специализированным процессором, который обрабатывает кадры по алгоритму моста независимо от процессоров других портов. За счет этого общая производительность коммутатора обычно намного выше производительности традиционного моста, имеющего один процессорный блок.

3. **Маршрутизатор** – *router* – более надежно и более эффективно, чем мосты, изолируют трафик отдельных частей сети друг от друга. Маршрутизаторы образуют логические сегменты посредством явной адресации, поскольку используют не плоские аппаратные, а составные числовые адреса. В этих адресах имеется поле номера сети, так что все компьютеры, у которых значение этого поля одинаково, принадлежат к одному сегменту, называемому в данном случае **подсетью** – *subnet.*

Кроме локализации трафика маршрутизаторы выполняют еще много других полезных функций. Так, маршрутизаторы могут работать в сети с замкнутыми контурами, при этом они осуществляют выбор наиболее рационального маршрута из нескольких возможных. Другой очень важной функцией маршрутизаторов является их способность связывать в единую сеть подсети, построенные с использованием разных сетевых технологий.

4. Кроме перечисленных устройств отдельные части сети может соединять **шлюз** – *gateway*. Обычно основной причиной, по которой в сети используют шлюз, является необходимость объединить сети с разными типами системного и прикладного программного обеспечения, а не желание локализовать трафик. Тем не менее, шлюз обеспечивает и локализацию трафика в качестве некоторого побочного эффекта.

Крупные сети практически никогда не строятся без логической структуризации. Для отдельных сегментов и подсетей характерны типовые однородные топологии базовых технологий, и для их объединения всегда используется оборудование, обеспечивающее локализацию трафика.

Линия связи (канал связи) состоит в общем случае из физической среды, по которой передаются электрические информационные сигналы, аппаратуры передачи данных и промежуточной аппаратуры.

Физическая среда передачи данных может представлять собой кабель, то есть набор проводов, изоляционных и защитных оболочек и соединительных разъемов, а также земную атмосферу или космическое пространство, через которые распространяются электромагнитные волны.

В зависимости от среды передачи данных линии связи разделяются на следующие:

– проводные (воздушные);

– кабельные (медные и волоконно-оптические);

– радиоканалы наземной и спутниковой связи.

Проводные (воздушные) линии связи представляют собой провода без каких-либо изолирующих или экранирующих оплеток, проложенные между столбами и висящие в воздухе. По таким линиям связи традиционно передаются телефонные или телеграфные сигналы, но при отсутствии других возможностей эти линии используются и для передачи компьютерных данных. Скоростные качества и помехозащищенность этих линий оставляют желать много лучшего. Сегодня проводные линии связи быстро вытесняются кабельными.

Кабельные линии представляют собой достаточно сложную конструкцию. Кабель состоит из проводников, заключенных в несколько слоев изоляции: электрической, электромагнитной, механической, а также, возможно, климатической. Кроме того, кабель может быть оснащен разъемами, позволяющими быстро выполнять присоединение к нему различного оборудования. В компьютерных сетях применяются три основных типа кабеля: кабели на основе скрученных пар медных проводов, коаксиальные кабели с медной жилой, а также волоконно-оптические кабели.

Скрученная пара проводов называется **витой парой** – *twisted pair*. Витая пара существует в экранированном (*shielded twisted pair, STP*) варианте, когда пара медных проводов обертывается в изоляционный экран, и неэкранированном (*unshielded twisted pair, UTP*), когда изоляционная обертка отсутствует. Скручивание проводов снижает влияние внешних помех на полезные сигналы, передаваемые по кабелю.

Коаксиальный кабель – *coaxial* – имеет несимметричную конструкцию и состоит из внутренней медной жилы и оплетки, отделенной от жилы слоем изоляции. Существует несколько типов коаксиального кабеля, отличающихся характеристиками и областями применения: для локальных сетей, для глобальных сетей, для кабельного телевидения и т. п.

Волоконно-оптический кабель – *optical fiber* – состоит из тонких волокон, по которым распространяются световые сигналы. Это наиболее качественный тип кабеля. Он обеспечивает передачу данных с очень высокой скоростью и к тому же лучше других типов передающей среды обеспечивает защиту данных от внешних помех.

Радиоканалы наземной и спутниковой связи образуются с помощью передатчика и приемника радиоволн. Существует большое количество различных типов радиоканалов, отличающихся как используемым частотным диапазоном, так и дальностью канала.

В компьютерных сетях сегодня применяются практически все описанные типы физических сред передачи данных, но наиболее перспективными являются волоконно-оптические. На них сегодня строятся как магистрали крупных территориальных сетей, так и высокоскоростные линии связи локальных сетей. Популярной средой является также витая пара, которая характеризуется отличным соотношением качества к стоимости, а также простотой монтажа. С помощью витой пары обычно подключают конечных абонентов сетей на расстояниях до 100 метров от концентратора. Спутниковые каналы и радиосвязь используются чаще всего в тех случаях, когда кабельные связи применить нельзя, например, при прохождении канала через малонаселенную местность или же для связи с мобильным пользователем сети.

Информационные сети можно классифицировать по различным признакам.

1. Уровень развития архитектуры ИС. По этому признаку классификации все ИС можно разделить на две большие группы:

– коммуникационные сети, т. е. такие, в которых применяемые средства рассчитаны на обеспечение связи и осуществление обмена информацией между территориально разделенными пользователями и абонентскими системами;

– информационно-вычислительные сети (ИВС), предоставляющие по запросам отдельных пользователей и систем те или иные информационные, вычислительные ресурсы и услуги.

Как правило, в ИС второй группы используется в качестве основы та или иная базовая коммуникационная сеть, через которую обеспечивается связь машин, выполняющих обработку информации. В этом отношении можно считать, что архитектура ИВС по уровню выше, чем архитектура коммуникационных ИС.

Уровень развития ИС определяет особенности сетевой архитектуры. К ним относятся: применяемые в ИС методы распределения информации и установления связей между взаимодействующими системами; виды, предоставляемых услуг; способы управления процессами; наличие средств защиты и обеспечения целостности данных и сохранности ресурсов; возможности организации связи с другими сетями и осуществления межсетевых переходов.

2. По способу управления процессами. В зависимости от вида средств, методов и алгоритмов управления можно выделить ИС с централизованным и распределенным управлением. При этом могут осуществляться как жесткие (фиксированные) алгоритмы управления ИС, так и гибкие (адаптивные) алгоритмы, учитывающие многочисленные внутренние и внешние по отношению к ИС факторы.

3. По наличию средств защиты, обеспечения целостности данных и сохранности ресурсов: ИС с системой защиты и ИС без системы защиты.

4. По возможности организации связи с другими сетями и осуществления межсетевых переходов. Если сеть может быть соединена с другими, то она называется открытой, если не может или не должна соединяться, то закрытой. Часто некоторые ИС целиком или только отдельные их части делаются специально закрытыми, чтобы ограничить доступ некоторой категории пользователей и тем самым защитить ее ресурсы.

5. Еще особенность сетевой архитектуры, которая учитывается при классификации ИС – это свойство однородности или неоднородности. Однородными считаются ИС, узлы которых состоят из однотипного оборудования и выполняют одинаковый набор функций, в противном случае сеть является неоднородной.

6. По основному целевому прикладному назначению ИС. По функционально-целевому и прикладному назначению существующие ИС можно разделить на две группы: общего пользования и специального назначения.

ИС общего пользования предназначены для разнообразных сфер применения независимо от конкретного содержания данных, которые эти ИС получают, передают, хранят и перерабатывают. Применяемые средства, структура и функциональные возможности таких ИС оказываются одинаковыми для многих случаев применения и обеспечивают широкие диапазоны услуг.

При использовании ИС специального назначения отметим следующие основные разновидности их: для автоматизированных систем управления (ИС АСУ); для систем автоматизированного проектирования (ИС САПР); автоматизированных систем научно-технической информации (ИС АСНТИ); для автоматизации процессов обучения (ИС АПО); бытового назначения (ИС БН).

7. Разделение по территориальному признаку. Здесь выделяют: глобальные (WAN), городские (MAN) и локальные (LAN) сети.

К **локальным сетям** – *local area networks (LAN)* – относят сети компьютеров, сосредоточенные на небольшой территории (обычно в радиусе не более 1–2 км). В общем случае локальная сеть представляет собой коммуникационную систему, принадлежащую одной организации. Из-за коротких расстояний в локальных сетях имеется возможность использования относительно дорогих высококачественных линий связи, которые позволяют, применяя простые методы передачи данных, достигать высоких скоростей обмена данными. В связи с этим услуги, предоставляемые локальными сетями, отличаются широким разнообразием и обычно предусматривают реализацию в режиме on-line.

Глобальные сети – *wide area networks (WAN)* – объединяют территориально рассредоточенные компьютеры, которые могут находиться в различных городах и странах. Так как прокладка высококачественных линий связи на большие расстояния обходится очень дорого, в глобальных сетях часто используются уже существующие линии связи, изначально предназначенные совсем для других целей. Например, многие глобальные сети строятся на основе телефонных и телеграфных каналов общего назначения. Из-за низких скоростей таких линий связи в глобальных сетях (десятки килобит в секунду) набор предоставляемых услуг обычно ограничивается передачей файлов, преимущественно не в оперативном, а в фоновом режиме, с использованием электронной почты. Для устойчивой передачи дискретных данных по некачественным линиям связи применяются методы и оборудование, существенно отличающиеся от методов и оборудования, характерных для локальных сетей. Как правило, здесь применяются сложные процедуры контроля и восстановления данных, так как наиболее типичный режим передачи данных по территориальному каналу связи связан со значительными искажениями сигналов.

Городские сети – *metropolitan area networks (MAN)* – являются менее распространенным типом сетей. Эти сети появились сравнительно недавно. Они предназначены для обслуживания территории крупного города. В то время как локальные сети наилучшим образом подходят для разделения ресурсов на коротких расстояниях и широковещательных передач, а глобальные сети обеспечивают работу на больших расстояниях, но с ограниченной скоростью и небогатым набором услуг, сети мегаполисов занимают некоторое промежуточное положение. Они используют цифровые магистральные линии связи, часто оптоволоконные, со скоростями от 45 Мбит/с, и предназначены для связи локальных сетей в масштабах города и соединения локальных сетей с глобальными.

Сети мегаполисов являются общественными сетями, и поэтому их услуги обходятся дешевле, чем построение собственной (частной) сети в пределах города.

8. Классификация по масштабу производственного подразделения. Еще одним популярным способом классификации сетей является их классификация по масштабу производственного подразделения, в пределах которого действует сеть. Различают сети отделов, сети кампусов и корпоративные сети.

Сети отделов – это сети, которые используются сравнительно небольшой группой сотрудников, работающих в одном отделе предприятия. Эти сотрудники решают некоторые общие задачи. Главной целью сети отдела является разделение локальных ресурсов, таких как приложения, данные, лазерные принтеры и модемы. Обычно сети отделов имеют один или два файловых сервера и не более тридцати пользователей. Сети отделов обычно не разделяются на подсети. В этих сетях локализуется большая часть трафика предприятия. Сети отделов обычно создаются на основе какой-либо одной сетевой технологии. Для такой сети характерен один или, максимум, два типа операционных систем. Чаще всего это сеть с выделенным сервером, хотя небольшое количество пользователей делает возможным использование одноранговых сетевых ОС.

Главными особенностями сетей кампусов являются следующие. Сети этого типа объединяют множество сетей различных отделов одного предприятия в пределах отдельного здания или в пределах одной территории, покрывающей площадь в несколько квадратных километров. При этом глобальные соединения в сетях кампусов не используются. Службы такой сети включают взаимодействие между сетями отделов, доступ к общим базам данных предприятия, доступ к общим факс-серверам, высокоскоростным модемам и высокоскоростным принтерам. В результате сотрудники каждого отдела предприятия получают доступ к некоторым файлам и ресурсам сетей других отделов. Важной службой, предоставляемой сетями кампусов, стал доступ к корпоративным базам данных независимо от того, на каких типах компьютеров они располагаются.

Именно на уровне сети кампуса возникают проблемы интеграции неоднородного аппаратного и программного обеспечения. Типы компьютеров, сетевых операционных систем, сетевого аппаратного обеспечения могут отличаться в каждом отделе. Отсюда вытекают сложности управления сетями кампусов. Администраторы должны быть в этом случае более квалифицированными, а средства оперативного управления сетью более совершенными.

Корпоративные сети называют также сетями масштаба предприятия, Сети масштаба предприятия (корпоративные сети) объединяют большое количество компьютеров на всех территориях отдельного предприятия. Они могут быть сложно связаны и покрывать город, регион или даже континент. Число пользователей и компьютеров может измеряться тысячами, а число серверов – сотнями, расстояния между сетями отдельных территорий могут оказаться такими, что становится необходимым использование глобальных связей. Для соединения удаленных локальных сетей и отдельных компьютеров в корпоративной сети применяются разнообразные телекоммуникационные средства, в том числе телефонные каналы, радиоканалы, спутниковая связь.

Непременным атрибутом такой сложной и крупномасштабной сети является высокая степень гетерогенности – нельзя удовлетворить потребности тысяч пользователей с помощью однотипных программных и аппаратных средств. В корпоративной сети обязательно будут использоваться различные типы компьютеров – от мэйнфреймов до персональных, несколько типов операционных систем и множество различных приложений. Неоднородные части корпоративной сети должны работать как единое целое, предоставляя пользователям по возможности прозрачный доступ ко всем необходимым ресурсам.

Суть сети – это соединение разного оборудования, а значит, проблема совместимости является одной из наиболее острых. Эту проблему решают стандарты взаимодействия открытых систем.

Каждая открытая система предназначена для выполнения двух задач – обработки данных и передачи данных. Поэтому она состоит из двух частей. Первая из них – прикладные процессы, предназначена для обработки данных и в первую очередь для нужд пользователей. Вторая часть – область взаимодействия, которая обеспечивает передачу данных между прикладными процессами, расположенными в различных системах.

В компьютерных сетях идеологической основой стандартизации является многоуровневый подход к разработке средств сетевого взаимодействия. Именно на основе этого подхода была разработана стандартная семиуровневая модель взаимодействия открытых систем.

Многоуровневый подход заключается в следующем. Все множество модулей разбивают на уровни. Уровни образуют иерархию, то есть имеются вышележащие и нижележащие уровни. Множество модулей, составляющих каждый уровень, сформировано таким образом, что для выполнения своих задач они обращаются с запросами только к модулям непосредственно примыкающего нижележащего уровня. С другой стороны, результаты работы всех модулей, принадлежащих некоторому уровню, могут быть переданы только модулям соседнего вышележащего уровня. Такая иерархическая декомпозиция задачи предполагает четкое определение функции каждого уровня и интерфейсов между уровнями. Интерфейс определяет набор функций, которые нижележащий уровень предоставляет вышележащему.

Сетевые компоненты, лежащие на одном уровне, но в разных узлах, обмениваются информацией в соответствии с некоторым протоколом. **Протокол** –

protocol – набор правил, которым следуют компьютеры и программы при обмене информацией. Существует масса различных протоколов, которые управляют всеми аспектами связи и передачи данных – от аппаратного до прикладного уровня, но все они сходны в том, что задают правила, делающие связь возможной.

Модули, реализующие протоколы соседних уровней и находящиеся в одном узле, также взаимодействуют друг с другом в соответствии с четко определенными правилами и с помощью стандартизованных форматов сообщений. Эти правила принято называть **интерфейсом**. Интерфейс определяет набор сервисов, предоставляемый данным уровнем соседнему уровню.

Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется **стеком коммуникационных протоколов.**

Под **топологией** – *topology* – информационной сети обычно понимается физическое расположение компьютеров сети друг относительно друга и способ соединения их линиями связи.

Важно отметить, что понятие топологии относится прежде всего к локальным сетям, в которых структуру связей можно легко проследить. В глобальных сетях структура связей обычно скрыта от пользователей и не слишком важна, так как каждый сеанс связи может производиться по своему пути.

Топология «Шина»

Шинная топология представляет собой топологию, в которой все устройства локальной сети подключаются к линейной сетевой среде передачи данных – шине или трассе.

Топология «Шина».

Каждое устройство независимо подключается к общему шинному кабелю с помощью специального разъема. Шинный кабель должен иметь на конце согласующий резистор, или терминатор, который поглощает электрический сигнал, не давая ему отражаться и двигаться в обратном направлении по шине.

Достоинства топологии:

– небольшое время установки сети;

– дешевизна (требуется меньше кабеля и сетевых устройств);

– простота настройки;

– выход из строя рабочей станции не отражается на работе сети.

Недостатки топологии:

– любые неполадки в сети, как обрыв кабеля, выход из строя терминатора полностью уничтожают работу всей сети;

– сложная локализация неисправностей;

– с добавлением новых рабочих станций падает производительность сети.

Топология «Кольцо»

При использовании кольцевой топологии все компьютеры сети подключаются последовательно друг к другу, образуя замкнутую сеть.

Топология «Кольцо».

В кольце, в отличие от других топологий, не используется конкурентный метод посылки данных, компьютер в сети получает данные от стоящего предыдущим в списке адресатов и перенаправляет их далее, если они адресованы не ему.

Достоинства топологии:

– простота установки;

– практически полное отсутствие дополнительного оборудования;

– возможность устойчивой работы без существенного падения скорости передачи при загрузке сети, поскольку использование маркера исключает возможность коллизий.

Недостатки топологии:

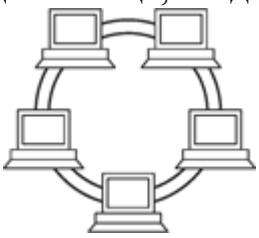
– выход из строя одной рабочей станции, и другие неполадки (обрыв кабеля), отражаются на работоспособности всей сети;

– сложность конфигурирования и настройки;

– сложность поиска неисправностей.

Топология «Двойное кольцо»

Эта топология использует два кольца, соединяющих компьютеры.

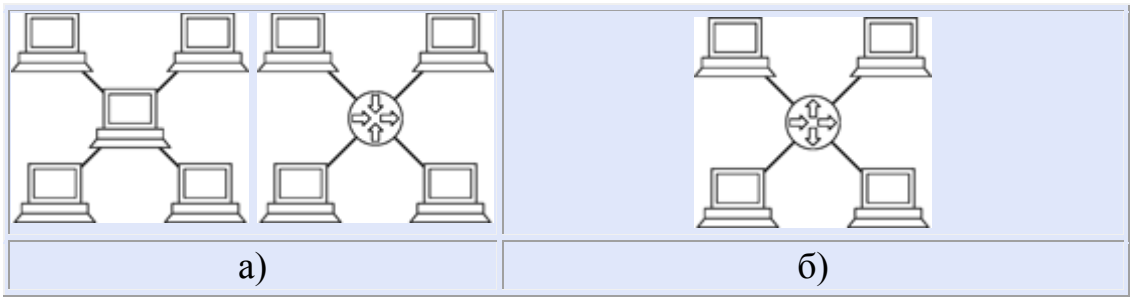


Топология «Двойное кольцо».

Два кольца образуют основной и резервный путь для передачи данных. Часто данные по первому кольцу передаются в одном направлении, а по второму в обратном. При выходе из строя одного кольца оно объединяется со вторым, и сеть продолжает функционировать.

Топология «Звезда»

При такой топологии все компьютеры сети присоединяются к одному центральному узлу с использованием отдельных линий связи.



а – активная «Звезда»; б – пассивная «Звезда»;

Топология «Звезда».

Передача данных осуществляется через центральный узел. При использовании концентрата в качестве центрального узла, только одна рабочая станция в сети в определенный момент времени может передавать данные. В случае применения коммутатора этот недостаток отсутствует.

Достоинства топологии:

– выход из строя одной рабочей станции не отражается на работе всей сети в целом;

– хорошая масштабируемость сети;

– легкий поиск неисправностей и обрывов в сети;

– высокая производительность сети (при условии правильного проектирования);

– гибкие возможности администрирования.

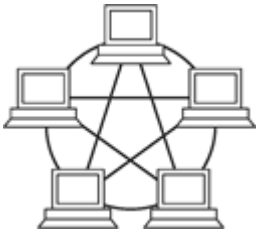
Недостатки топологии:

– выход из строя центрального концентратора обернётся неработоспособностью сети (или сегмента сети) в целом;

– для прокладки сети зачастую требуется больше кабеля, чем для большинства других топологий;

– конечное число рабочих станций в сети (или сегменте сети) ограничено количеством портов в центральном концентраторе.

Ячеистая топология – базовая полносвязная топология компьютерной сети, в которой каждая рабочая станция сети соединяется со всеми другими рабочими станциями этой же сети.



Ячеистая топология.

Достоинства топологии:

– высокая отказоустойчивость;

– повышенная пропускная способность;

– высокий уровень безопасности, т. к. поток информации идет от компьютера-отправителя к получателю напрямую.

Недостатки топологии:

– сложность настройки;

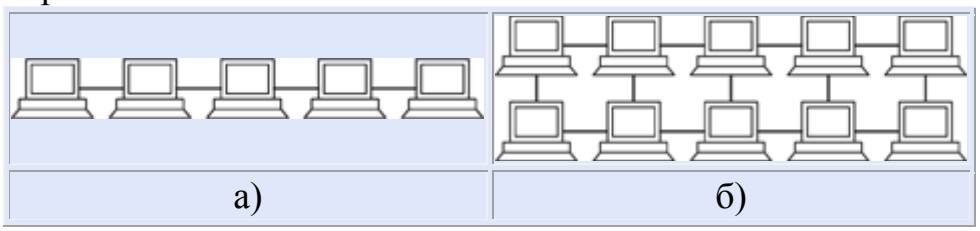
– избыточный расход кабеля;

– потребность наличия нескольких сетевых интерфейсов на компьютерах сети.

Топология «Решетка»

Это топология, в которой узлы образуют регулярную многомерную решетку. При этом каждое ребро решетки параллельно ее оси и соединяет два смежных узла вдоль этой оси.

Одномерная решётка – это цепь, соединяющая два внешних узла (имеющие лишь одного соседа) через некоторое количество внутренних (у которых по два соседа – слева и справа). При соединении обоих внешних узлов получается кольцевая топология. Двух- и трехмерные решетки используются в архитектуре суперкомпьютеров.



а) б)

а – одномерная «Решетка»; б – двумерная «Решетка»;
Топология «Решетка».

Достоинства топологии:

– высокая надежность;

– высокая отказоустойчивость.

Недостатки топологии:

– сложность реализации.

3. Сетевые операционные системы

Сетевые операционные системы

(Network Operating System – NOS) – это комплекс программ, обеспечивающих обработку, хранение и передачу данных в сети.

Сетевая операционная система выполняет функции прикладной платформы, предоставляет разнообразные виды сетевых служб и поддерживает работу прикладных процессов, выполняемых в абонентских системах. Сетевые операционные системы используют клиент-серверную, либо одноранговую архитектуру. Компоненты NOS располагаются на всех рабочих станциях, включенных в сеть.

NOS определяет взаимосвязанную группу протоколов верхних уровней, обеспечивающих выполнение основных функций сети. К ним, в первую очередь, относятся:

1. адресация объектов сети;
2. функционирование сетевых служб;
3. обеспечение безопасности данных;
4. управление сетью.

При выборе NOS необходимо рассматривать множество факторов. Среди них:

- набор сетевых служб, которые предоставляет сеть;

- возможность наращивания имен, определяющих хранимые данные и прикладные программы;
- механизм рассредоточения ресурсов по сети;
- способ модификации сети и сетевых служб;
- надежность функционирования и быстродействие сети;
- используемые или выбираемые физические средства соединения;
- типы компьютеров, объединяемых в сеть, их операционные системы;
- предлагаемые системы, обеспечивающие управление сетью;
- используемые средства защиты данных;
- совместимость с уже созданными прикладными процессами;
- число серверов, которое может работать в сети;
- перечень ретрансляционных систем, обеспечивающих сопряжение локальных сетей с различными территориальными сетями;
- способ документирования работы сети, организация подсказок и поддержек.

Функции и характеристики сетевых операционных систем (ОС).

Различают ОС со встроенными сетевыми функциями и оболочки над локальными ОС. По другому признаку классификации различают сетевые ОС одноранговые и функционально несимметричные (для систем «клиент/сервер»).

Основные функции сетевой ОС:

1) управление каталогами и файлами;
2) управление ресурсами;
3) коммуникационные функции;
4) защита от несанкционированного доступа;
5) обеспечение отказоустойчивости;
6) управление сетью.

Управление каталогами и файлами в сетях заключается в обеспечении доступа к данным, физически расположенным в других узлах сети. Управление осуществляется с помощью специальной сетевой файловой системы. Файловая система позволяет обращаться к файлам путем применения привычных для локальной работы языковых средств. При обмене файлами должен быть обеспечен необходимый уровень конфиденциальности обмена (секретности данных).

Управление ресурсами включает обслуживание запросов на предоставление ресурсов, доступных по сети.

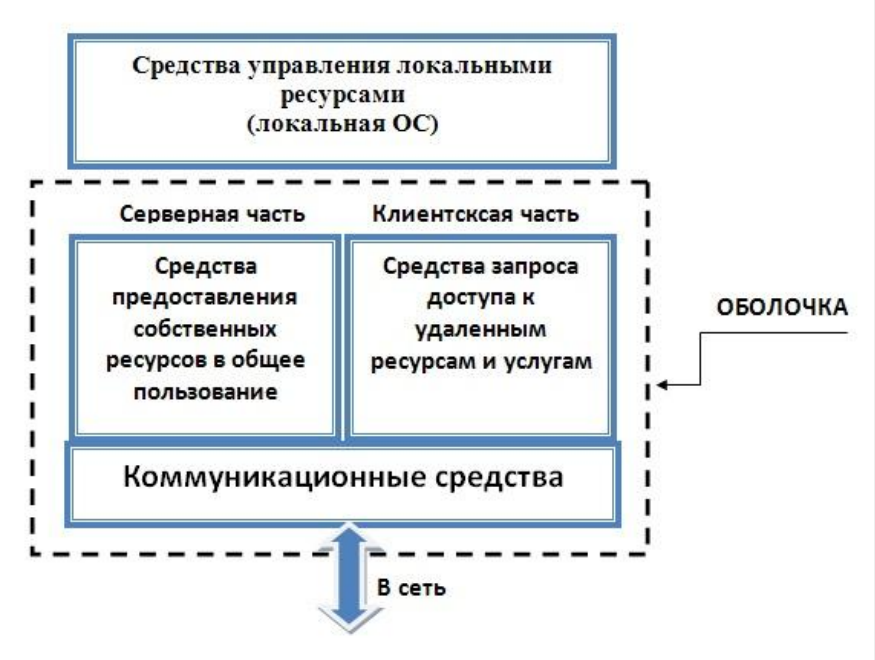
Коммуникационные функции обеспечивают адресацию, буферизацию, выбор направления для движения данных в разветвленной сети (маршрутизацию), управление потоками данных и др. Защита от несанкционированного доступа – важная функция, способствующая поддержанию целостности данных и их конфиденциальности. Средства защиты могут разрешать доступ к определенным данным только с некоторых терминалов, в оговоренное время, определенное число раз и т. п. У каждого пользователя в корпоративной сети могут быть свои права доступа с ограничением совокупности доступных директорий или списка возможных действий, например, может быть запрещено изменение содержимого некоторых файлов.

Отказоустойчивость характеризуется сохранением работоспособности системы при воздействии дестабилизирующих факторов. Отказоустойчивость обеспечивается применением для серверов автономных источников питания, отображением или дублированием информации в дисковых накопителях. Под отображением обычно понимают наличие в системе двух копий данных с их расположением на разных дисках, но подключенных к одному контроллеру. Дублирование отличается тем, что для каждого из дисков с копиями используются разные контроллеры. Очевидно, что дублирование более надежно. Дальнейшее повышение отказоустойчивости связано с дублированием серверов, что однако требует дополнительных затрат на приобретение оборудования.

Управление сетью связано с применением соответствующих протоколов управления. Программное обеспечение управления сетью обычно состоит из менеджеров и агентов. Менеджером называется программа, вырабатывающая сетевые команды. Агенты представляют собой программы, расположенные в различных узлах сети. Они выполняют команды менеджеров, следят за состоянием узлов, собирают информацию о параметрах их функционирования, сигнализируют о происходящих событиях, фиксируют аномалии, следят за трафиком, осуществляют защиту от вирусов. Агенты с достаточной степенью интеллектуальности могут участвовать в восстановлении информации после сбоев, в корректировке параметров управления и т. п.

Структура сетевой операционной системы

Сетевая операционная система составляет основу любой вычислительной сети. Каждый компьютер в сети автономен, поэтому под сетевой операционной системой в широком смысле понимается совокупность операционных систем отдельных компьютеров, взаимодействующих с целью обмена сообщениями и разделения ресурсов по единым правилам – протоколам. В узком смысле сетевая ОС – это операционная система отдельного компьютера, обеспечивающая ему возможность работать в сети.



Структура сетевой ОС

В соответствии со структурой, в сетевой операционной системе отдельной машины можно выделить несколько частей.

1. Средства управления локальными ресурсами компьютера: функции распределения оперативной памяти между процессами, планирования и диспетчеризации процессов, управления процессорами, управления периферийными устройствами и другие функции управления ресурсами локальных ОС.

2. Средства предоставления собственных ресурсов и услуг в общее пользование – серверная часть ОС (сервер). Эти средства обеспечивают, например, блокировку файлов и записей, ведение справочников имен сетевых ресурсов; обработку запросов удаленного доступа к собственной файловой системе и базе данных; управление очередями запросов удаленных пользователей к своим периферийным устройствам.

3. Средства запроса доступа к удаленным ресурсам и услугам – клиентская часть ОС (редиректор). Эта часть выполняет распознавание и перенаправление в сеть запросов к удаленным ресурсам от приложений и пользователей. Клиентская часть также осуществляет прием ответов от серверов и преобразование их в локальный формат, так что для приложения выполнение локальных и удаленных запросов неразличимо.

4. Коммуникационные средства ОС, с помощью которых происходит обмен сообщениями в сети. Эта часть обеспечивает адресацию и буферизацию сообщений, выбор маршрута передачи сообщения по сети, надежность передачи и т. п., то есть является средством транспортировки сообщений.

Клиентское программное обеспечение

Для работы с сетью на клиентских рабочих станциях должно быть установлено клиентское программное обеспечение. Это программное обеспечение обеспечивает доступ к ресурсам, расположенным на сетевом сервере. Тремя наиболее важными компонентами клиентского программного обеспечения являются редиректоры (redirector), распределители (designator) и имена UNC (UNC pathnames).

Редиректоры

Редиректор – сетевое программное обеспечение, которое принимает запросы ввода/вывода для удаленных файлов, именованных каналов или почтовых слотов и затем пере-назначает их сетевым сервисам другого компьютера. Редиректор перехватывает все запросы, поступающие от приложений, и анализирует их.

Фактически существуют два типа редиректоров, используемых в сети:

- клиентский редиректор (client redirector)
- серверный редиректор (server redirector).

Оба редиректора функционируют на представительском уровне модели OSI. Когда клиент делает запрос к сетевому приложению или службе, редиректор перехватывает этот запрос и проверяет, является ли ресурс локальным (находящимся на запрашивающем компьютере) или удаленным (в сети). Если редиректор определяет, что это локальный запрос, он направляет запрос центральному процессору для немедленной обработки. Если запрос предназначен для сети, редиректор направляет запрос по сети к соответствующему серверу. По существу, редиректоры скрывают от пользователя сложность доступа к сети. После того как сетевой

ресурс определен, пользователи могут получить к нему доступ без знания его точного расположения.

Распределители

Распределитель (designator) представляет собой часть программного обеспечения, управляющую присвоением букв накопителя (drive letter) как локальным, так и удаленным сетевым ресурсам или разделяемым дисководам, что помогает во взаимодействии с сетевыми ресурсами. Когда между сетевым ресурсом и буквой локального накопителя создана ассоциация, известная также как отображение дисковода (mapping a drive), распределитель отслеживает присвоение такой буквы дисковода сетевому ресурсу. Затем, когда пользователь или приложение получат доступ к диску, распределитель заменит букву дисковода на сете-вой адрес ресурса, прежде чем запрос будет послан редиректору.

Имена UNC

Редиректор и распределитель являются не единственными методами, используемыми для доступа к сетевым ресурсам. Большинство современных сетевых операционных систем, так же как и Windows 95, 98, NT, распознают имена UNC (Universal Naming Convention — Универсальное соглашение по наименованию). UNC представляют собой стандартный способ именования сетевых ресурсов. Эти имена имеют форму \\Имя_сервера\имя_ресурса. Способные работать с UNC приложения и утилиты командной строки используют имена UNC вместо отображения сетевых дисков.

Серверное программное обеспечение

Для того чтобы компьютер мог выступать в роли сетевого сервера необходимо установить серверную часть сетевой операционной системы, которая позволяет поддерживать ресурсы и распространять их среди сетевых клиентов. Важным вопросом для сетевых серверов является возможность ограничить доступ к сетевым ресурсам. Это называется сетевой защитой (network security). Она предоставляет средства управления над тем, к каким ресурсам могут получить доступ пользователи, степень этого доступа, а также, сколько пользователей смогут получить такой доступ одновременно. Этот контроль обеспечивает конфиденциальность и защиту и поддерживает эффективную сетевую среду.

В дополнение к обеспечению контроля над сетевыми ресурсами сервер выполняет следующие функции:

- предоставляет проверку регистрационных имен (logon identification) для пользователей;
- управляет пользователями и группами;
- хранит инструменты сетевого администрирования для управления, контроля и аудита;
- обеспечивает отказоустойчивость для защиты целостности сети.

Клиентское и серверное программное обеспечение

Некоторые из сетевых операционных систем, в том числе Windows, имеют программные компоненты, обеспечивающие компьютеру как клиентские, так и серверные возможности. Это позволяет компьютерам поддерживать и использовать сетевые ресурсы и преобладает в одноранговых сетях. В общем, этот тип се-

тевых операционных систем не так мощен и надежен, как законченные сетевые операционные системы.

Главное преимущество комбинированной клиентско-серверной сетевой операционной системы заключается в том, что важные ресурсы, расположенные на отдельной рабочей станции, могут быть разделены с остальной частью сети.

Недостаток состоит в том, что если рабочая станция поддерживает много активно используемых ресурсов, она испытывает серьезное падение производительности. Если такое происходит, то необходимо перенести эти ресурсы на сервер для увеличения общей производительности.

В зависимости от функций, возлагаемых на конкретный компьютер, в его операционной системе может отсутствовать либо клиентская, либо серверная части.

Если выдан запрос к ресурсу данного компьютера, то он переадресовывается локальной операционной системе. Если же это запрос к удаленному ресурсу, то он переправляется в клиентскую часть, где преобразуется из локальной формы в сетевой формат, и передается коммуникационным средствам. Серверная часть ОС компьютера 2 принимает запрос, преобразует его в локальную форму и передает для выполнения своей локальной ОС. После того, как результат получен, сервер обращается к транспортной подсистеме и направляет ответ клиенту, выдавшему запрос. Клиентская часть преобразует результат в соответствующий формат и адресует его тому приложению, которое выдало запрос.

Требования к современным операционным системам

Главным требованием, предъявляемым к операционной системе, является выполнение ею основных функций эффективного управления ресурсами и обеспечение удобного интерфейса для пользователя и прикладных программ. Современная ОС, как правило, должна поддерживать мультипрограммную обработку, виртуальную память, свопинг, многооконный графический интерфейс пользователя, а также выполнять многие другие необходимые функции и услуги. Кроме этих требований функциональной полноты к операционным системам предъявляются не менее важные эксплуатационные требования, которые перечислены ниже.

Расширяемость.

В то время как аппаратная часть компьютера устаревает за несколько лет, полезная жизнь операционных систем может измеряться десятилетиями. Примером может служить ОС UNIX. Поэтому операционные системы всегда изменяются со временем эволюционно, и эти изменения более значимы, чем изменения аппаратных средств. Изменения ОС обычно заключаются в приобретении ею новых свойств, например поддержке новых типов внешних устройств или новых сетевых технологий. Если код ОС написан таким образом, что дополнения и изменения могут вноситься без нарушения целостности системы, то такую ОС называют расширяемой. Расширяемость достигается за счет модульной структуры ОС, при которой программы строятся из набора отдельных модулей, взаимодействующих только через функциональный интерфейс.

Переносимость.

В идеале код ОС должен легко переноситься с процессора одного типа на процессор другого типа и с аппаратной платформы (которые различаются не

только типом процессора, но и способом организации всей аппаратуры компьютера) одного типа на аппаратную платформу другого типа. Переносимые ОС имеют несколько вариантов реализации для разных платформ, такое свойство ОС называют также многоплатформенностью.

Совместимость.

Существует несколько «долгоживущих» популярных операционных систем (разновидности UNIX, Windows, Windows Server), для которых наработана широкая номенклатура приложений. Некоторые из них пользуются широкой популярностью. Поэтому для пользователя, переходящего по тем или иным причинам с одной ОС на другую, очень привлекательна возможность запуска в новой операционной системе привычного приложения. Если ОС имеет средства для выполнения прикладных программ, написанных для других операционных систем, то про нее говорят, что она обладает совместимостью с этими ОС. Следует различать совместимость на уровне двоичных кодов и совместимость на уровне исходных текстов. Понятие совместимости включает также поддержку пользовательских интерфейсов других ОС.

Надежность и отказоустойчивость.

Система должна быть защищена как от внутренних, так и от внешних ошибок, сбоев и отказов. Ее действия должны быть всегда предсказуемыми, а приложения не должны иметь возможности наносить вред ОС. Надежность и отказоустойчивость ОС прежде всего определяются архитектурными решениями, положенными в ее основу, а также качеством ее реализации (отлаженностью кода). Кроме того, важно, включает ли ОС программную поддержку аппаратных средств обеспечения отказоустойчивости, таких, например, как дисковые массивы или источники бесперебойного питания.

Безопасность.

Современная ОС должна защищать данные и другие ресурсы вычислительной системы от несанкционированного доступа. Чтобы ОС обладала свойством безопасности, она должна как минимум иметь в своем составе средства аутентификации – определения легальности пользователей, авторизации – предоставления легальным пользователям дифференцированных прав доступа к ресурсам, аудита – фиксации всех «подозрительных» для безопасности системы событий. Свойство безопасности особенно важно для сетевых ОС. В таких ОС к задаче контроля доступа добавляется задача защиты данных, передаваемых по сети.

Производительность.

Операционная система должна обладать настолько хорошим быстродействием и временем реакции, насколько это позволяет аппаратная платформа. На производительность ОС влияет много факторов, среди которых основными являются архитектура ОС, многообразие функций, качество программирования кода, возможность исполнения ОС на высокопроизводительной (многопроцессорной) платформе.

Выбор сетевой операционной системы

При выборе сетевой операционной системы необходимо учитывать:

- совместимость оборудования;

- тип сетевого носителя;
- размер сети;
- сетевую топологию;
- требования к серверу;
- операционные системы на клиентах и серверах;
- сетевая файловая система;
- соглашения об именах в сети;
- организация сетевых устройств хранения.

В настоящее время наибольшее распространение получили две основные сетевые ОС – UNIX и Windows.

ОС UNIX применяют преимущественно в крупных корпоративных сетях, поскольку эта система характеризуется высокой надежностью, возможностью легкого масштабирования сети. В Unix имеется ряд команд и поддерживающих их программ для работы в сети.

Во-первых, это команды ftp, telnet, реализующие файловый обмен и эмуляцию удаленного узла на базе протоколов TCP/IP. Во-вторых, протокол, команды и программы UUCP, разработанные с ориентацией на асинхронную модемную связь по телефонным линиям между удаленными Unix-узлами в корпоративных и территориальных сетях.

ОС Windows Server обеспечивает работу в сетях «клиент/сервер». Windows обычно применяют в средних по масштабам сетях.

Операционная система UNIX – многопользовательская, многозадачная операционная система, способная функционировать на различных аппаратных платформах. В микроядро ОС UNIX встроен модуль, выполняющий протокол управления передачей/межсетевой протокол (протокол TCP/IP).

Операционная система Linux – сетевая операционная система, ядро которой разработано на базе операционной системы Unix. Linux распространяется с открытыми исходными кодами и применяется для создания серверов в вычислительных сетях и в Интернете.

Сетевая операционная система NetWare – разработанная корпорацией Novell сетевая операционная система, которая использует одноранговую архитектуру или архитектуру клиент-сервер.

4. Средства реализации межсетевого взаимодействия

При описании практически любого взаимодействия можно выделять различные уровни. Например, представьте себе, что двум людям, проживающим в разных населенных пунктах, необходимо обмениваться какой-либо информацией, и они используют для этого традиционный способ посылки писем. Уже во взаимодействии такого рода можно выделить несколько уровней:

- уровень пользователей, обменивающихся письмами, и использующих для этой цели почтовую службу;
- уровень почтовой службы, осуществляющей пересылку корреспонденции между почтовыми отделениями населенных пунктов и использующей для работы услуги транспортной сети;

- уровень транспортной сети, обеспечивающий доставку грузов по путям сообщения между населенными пунктами;
- уровень путей сообщения, обеспечивающий возможность физической доставки грузов между населенными пунктами.

В случае, если не существует прямых путей сообщения между населенными пунктами, к этой схеме между уровнями почтовой службы и транспортной сети добавляется еще один уровень – уровень отделений по перевозке почты, обеспечивающих правильную перегрузку почтовых отправлений на транспортных узлах, а также выбор альтернативных путей пересылки в случае выхода из строя транспортных линий.

Разделение процесса взаимодействия на уровни позволяет функционально изолировать различные средства, участвующие в этом процессе по принципу – «каждый занимается своим делом». Это позволяет обеспечить достаточную гибкость при расширении функциональности этих средств. Так, например, выделение уровня транспортной сети, позволяет при необходимости обеспечить транспортировку между населенными пунктами не только почтовых грузов, но и пассажиров, не требуя для этого перестройки путей сообщения. Выделение почтовой службы обеспечивает возможность пересылки не только писем, но и посылок, переводов и т. п., используя стандартные средства транспортной сети и опосредованно – существующие пути сообщения.

Взаимодействие в компьютерных сетях также можно описывать с помощью уровней. В настоящее время для этих целей широко используется так называемая модель взаимодействия открытых систем (Open Systems Interconnection, OSI).

Модель сетевого взаимодействия

В 1984 году Международной Организацией по Стандартизации (International Standard Organization, ISO) была разработана **модель взаимодействия открытых систем** (Open Systems Interconnection, OSI). Модель представляет собой международный стандарт для проектирования сетевых коммуникаций и предполагает уровневый подход к построению сетей. Каждый уровень модели обслуживает различные этапы процесса взаимодействия. Посредством деления на уровни сетевая модель OSI упрощает совместную работу оборудования и программного обеспечения. Модель OSI разделяет сетевые функции на семь уровней: прикладной, уровень представления, сессионный, транспортный, сетевой, канальный и физический.

Ниже дается краткая характеристика уровней модели:

- **Физический уровень** (Physical layer) определяет способ физического соединения компьютеров в сети. Функциями средств, относящихся к данному уровню, являются побитовое преобразование цифровых данных в сигналы, передаваемые по физической среде (например, по кабелю), а также собственно передача сигналов.
- **Канальный уровень** (Data Link layer) отвечает за организацию передачи данных между абонентами через физический уровень, поэтому на данном уровне предусмотрены средства адресации, позволяющие однозначно идентифицировать отправителя и получателя во всем множестве абонентов, подключенных к обще ли-

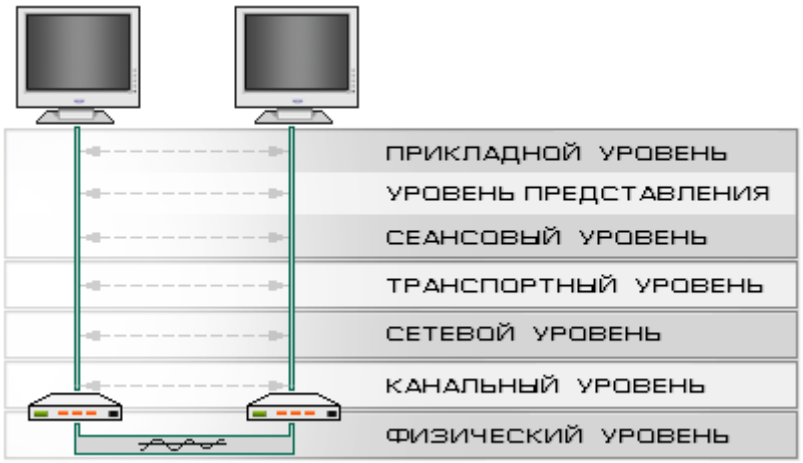
нии связи. В функции данного уровня также входит упорядочивание передачи с целью параллельного использования одной линии связи несколькими парами абонентов. Кроме того, средства канального уровня обеспечивают проверку ошибок, которые могут возникать при передаче данных физическим уровнем.

- **Сетевой уровень** (Network layer) обеспечивает доставку данных между компьютерами сети, представляющей собой объединение различных физических сетей. Данный уровень предполагает наличие средств логической адресации, позволяющих однозначно идентифицировать компьютер в объединенной сети. Одной из главных функций, выполняемых средствами данного уровня, является целенаправленная передача данных конкретному получателю.
- **Транспортный уровень** (Transport layer) реализует передачу данных между двумя программами, функционирующими на разных компьютерах, обеспечивая при этом отсутствие потерь и дублирования информации, которые могут возникать в результате ошибок передачи нижних уровней. В случае, если данные, передаваемые через транспортный уровень, подвергаются фрагментации, то средства данного уровня гарантируют сборку фрагментов в правильном порядке.
- **Сессионный (или сеансовый) уровень** (Session layer) позволяет двум программам поддерживать продолжительное взаимодействие по сети, называемое **сессией** (session) или **сеансом**. Этот уровень управляет установлением сеанса, обменом информацией и завершением сеанса. Он также отвечает за идентификацию, позволяя тем самым только определенным абонентам принимать участие в сеансе, и обеспечивает работу служб безопасности с целью упорядочивания доступа к информации сессии.
- **Уровень представления** (Presentation layer) осуществляет промежуточное преобразование данных исходящего сообщения в общий формат, который предусмотрен средствами нижних уровней, а также обратное преобразование входящих данных из общего формата в формат, понятный получающей программе.
- **Прикладной уровень** (Application layer) предоставляет высокоуровневые функции сетевого взаимодействия, такие, как передача файлов, отправка сообщений по электронной почте и т. п.

Основные принципы уровневого взаимодействия

При уровневой организации процесса взаимодействия должны соблюдаться следующие требования:

- компоненты одного уровня одной системы могут взаимодействовать с компонентами только того же уровня другой системы;
- в рамках одной системы компоненты какого-либо уровня могут взаимодействовать только с компонентами смежных (вышележащего и нижележащего) уровней.



Порядок уровневого взаимодействия

Набор правил, определяющих порядок взаимодействия средств, относящихся к одному и тому же уровню и функционирующих в разных системах, называется **протоколом** (protocol). Правила взаимодействия между собой средств, относящихся к смежным уровням и функционирующих в одной системе, называются **интерфейсом** (interface).

Практическая реализация уровневого взаимодействия

На практике протоколы и интерфейсы регламентируют технические требования, предъявляемые к программным и аппаратным средствам. Программные (аппаратные) модули, предназначенные для обеспечения практического взаимодействия, определяемого тем или иным протоколом (или интерфейсом), обычно называют **реализацией** протокола (или интерфейса)

Хотя различные компоненты, относящиеся к различным уровням сетевой модели формально должны быть функционально независимыми друг от друга, при практической разработке протоколов такая независимость не всегда выдерживается. Это объясняется тем, что попытка добиться точного соответствия эталонной модели может привести к неэффективности работы программно-аппаратного обеспечения, реализующего протокол. В настоящее время наблюдается два типа отклонений, возникающих при реализации уровневого взаимодействия:

- функции некоторых уровней могут объединяться одним протоколом и наоборот, – функции одного уровня могут делиться между различными протоколами;
- функционирование протокола какого-либо уровня подразумевают использование только определенных протоколов нижележащего уровня.

Поэтому разработка практических методов сетевого взаимодействия, как правило, подразумевает разработку не отдельных протоколов, а целых наборов протоколов. Такие наборы обычно включают в себя протоколы, относящиеся к нескольким смежным уровням эталонной модели OSI, и называются **стеками** (или семействами, наборами) **протоколов** (protocol stack, protocol suite). Наиболее известным стеком протоколов, обеспечивающим взаимодействие в сети Интернет, является стек протоколов TCP/IP.

Поскольку при реализации протоколов допускаются отклонения от эталонной модели, стеки протоколов могут предполагать собственную схему деления на

уровни. В частности, стек протоколов TCP/IP разделяет весь процесс сетевого взаимодействия на четыре уровня. На предложенном ниже рисунке показано соответствие уровней модели OSI и уровней стека TCP/IP.

Уровни модели OSI	Уровни стека TCP/IP
прикладной представления сессионный	уровень приложения
транспортный	транспортный уровень
сетевой	межсетевой уровень
канальный физический	уровень сетевого интерфейса

Соответствие уровней модели OSI и уровней стека TCP/IP

5. Перспективные направления развития и проблемы информационных сетей

Сегодня невозможно представить нашу жизнь без Интернета и информационных технологий. Они прочно вошли в нашу жизнь, значительно упростив ее. С развитием информационных технологий нам становятся доступны новые инструменты, которые делают привычные нам процессы быстрее, удобнее, и дешевле. Однако, те изменения, которые мы сейчас видим – это только верхушка айсберга. Сетевые технологии находятся лишь в начале пути своего роста и по-настоящему большие инновации ждут нас впереди. Итак, какую эволюцию на ближайшие десятилетия можно прогнозировать уже сегодня, видя, в каком направлении идет развитие компьютерных сетей и Интернета?

1. Будет расти охват аудитории, Интернет появится в самых отдаленных местах планеты. К концу 2012 г. число пользователей Интернет по всему миру достигло 2,4 миллиард пользователей по всему миру. К 2020 г. по прогнозам Национального Научного Фонда США число пользователей Интернет возрастет до 5 млрд. Интернет станет более распределен географически. Самый большой прирост пользователей в ближайшие 10 лет будет происходить за счет жителей развивающихся стран в Африке (сейчас используют не более 7 %), Азии (около 19 %) и Среднего Востока (Middle East) (около 28 %). Для сравнение в настоящее время более 72 % жителей Северной Америки используют Интернет. Этот тренд означает, что Интернет к 2020 году не только достигнет отдаленных мест по всему миру, но и будет поддерживать гораздо больше языков и не только привычную нам кодировочную систему ASCII. Российских пользователей Интернет, по данным Минкомсвязи РФ, на начало 2012 года было 70 млн. чел. По этому показателю Россия вышла на первое место в Европе и на шестое место в мире. Согласно результатам исследования агентства РБК.research, уровень проникновения Интернета в России в 2018 году превысит отметку в 80 %.

2. В информационных технологиях начинается эпоха программного обеспечения. Сейчас мы переживаем этап интеллектуализации «железа», когда программное обеспечение становится важнее самого оборудования. Индустрия ПО будет расти большими темпами: в 2010г. ежегодный темп роста софта был не менее 6 %, 2015 г. объемы рынка достигнут $365 млрд, четверть из которых приходится на рынок бизнес-приложений. Рынок «железа» будет сокращаться: объем рынка в 2013 г. составил $608 млрд, темп роста с 2008 по 2013 отрицательный – 0,7 %. До 2018 г. прогнозируется рост на 2,1 % преимущественно за счет роста рынка ПК (он будет расти на 7,5 %) и периферийных устройств (принтеры, сканеры и т. д.). XXI век – это век беспроводных технологий. Только за 2009 г. число абонентов мобильной широкополосной связи (3G, WiMAX и другие технологии высокоскоростной передачи данных) увеличилось на 85 %. К 2014 г. прогнозируют, что 2,5 млрд людей по всему миру будут использовать мобильный широкополосный доступ.

3. Увеличивается скорость передачи данных и пропускная способность. На сегодняшний день скорость передачи данных в хороших компьютерах – 40 Гбит/сек. Для примера, 4 тома романа «Война и Мир» Л. Толстого – это порядка 40 Мбит, т. е. в 1000 раз меньше! Передать эти 4 тома можно менее, чем за 1 микросекунду. Но, в ближайшем будущем можно будет передавать данные со скоростью света. Уже сегодня есть технология WiGik, которая позволяет на расстоянии нескольких километров передавать информацию со скорость 7 ГБит /сек. методом кодирования информации на физическом уровне. Так же и с пропускной способностью. Согласно данным компании Cisco, сегодня одновременно в Skype работает свыше 35 млн. пользователей, в Facebook – свыше 200 млн, каждую минуту на YouTube загружают 72 часа видео. Эксперты прогнозируют, что к 2015 году количество устройств в сети будет в два раза выше, чем население планеты. К 2014 году около 80 % этого трафика будет составлять видео трафик. Изображения и видео файлы, обмен которыми постоянно происходит во «всемирной паутине», требуют более высокой пропускной способности. И технологии будут развиваться в этом направлении. Пользователи будут общаться, и обмениваться информацией посредством видео и голоса в режиме реального времени. Все больше и больше появляется сетевых приложений, требующих взаимодействия в рольном времени.

4. Семантический WEB. Мы правомерно движемся в сторону «семантического интернета», в котором информации придается точно определенный смысл, что позволяет компьютерам «понимать» и обрабатывать ее на семантическом уровне. Сегодня компьютеры работают на синтаксическом уровне, на уровне знаков, они считывают и обрабатывают информацию по внешним признакам. Термин «семантическая паутина» был впервые введён сэром Тимом Бернерсом-Ли (один из изобретателей Всемирной паутины) в журнале «Scientific American». Семантический WEB позволит находить информацию по поиску: «Найти информацию о животных, использующих звуковую локацию, но не являющихся ни летучей мышью ни дельфином», например.

5. Новые объекты передачи. Благодаря развитию новых технологий можно будет передавать через компьютерные сети то, что раньше казалось невозможным. Например – запах. Машина анализирует молекулярный состав воздуха в одной точке и передает эти данные по сети. В другой точке сети этот молекулярный состав, т.е. запах синтезируется. Прототип подобного устройства уже выпустила американская компания Mint Foundry, называется она Olly, пока не поступила в свободную продажу. Однако скоро мы сможем увидеть воплощение этих возможностей в повседневной жизни.

6. Интернет станет сетью вещей, а не только компьютеров. Сегодня в сети Интернет насчитывается уже свыше 700 миллионов компьютеров (по данным CIA World Factbook 2012). Каждый год у пользователя увеличивается число устройств, который выходят в сеть: компьютеры, телефоны, планшеты и т. д. Уже сегодня количество IP-адресов превышает количество населения Земли (IP-адреса нужны для работы бытовых приборов). С новой архитектурой компьютерных сетей наступит эра «интернет-вещей». Вещи и предметы будут взаимодействовать через сети, это откроет большие возможности для всех сфер жизнедеятельности человека. Одна из ближайших разработок – это «умная пыль» – датчики, разбросанные на большой территории, собирающие информацию. Национальный Научный Фонд США прогнозирует, что около миллиардов датчиков на зданиях, мостах, дорогах будут подключены к Интернет для таких целей, как мониторинг использования электричества, для обеспечения безопасности и т. д. В целом ожидается, что к 2020 г. количество интернет-подключенных датчиков будет на порядок больше, чем количество пользователей. В продолжение данной мысли можно привести размышления Винтона Грэя Сёрфа (американский ученый-математик, считается одним из изобретателей протокола TCP/IP, вице-президент компании Google): «Предположим, что все продукты, которые вы кладете в холодильник, снабжены специальным штрих-кодом или микрочипом так, чтобы холодильник фиксировал все, что вы поместили в него. В таком случае, находясь в университете или на работе, вы можете просматривать эту информацию со своего телефона, смотреть разные варианты рецептов, а холодильник предложил бы вам, что стоит сегодня приготовить. Если расширить эту идею, то получится приблизительно следующая картина. Вы идете в магазин, и пока вы там находитесь, у вас звонит мобильный телефон – это звонит вам холодильник, который советует, что именно стоит купить». «Умный интернет» превратит социальные сети (в том виде, что мы имеем сегодня) в социальные медиа-системы. В помещениях будут установлены камеры и различные датчики. Через собственный аккаунт можно будет кормить питомцев и запускать стиральную машину, например.

7. Роботизация общества. Уже сегодня мы знаем примеры беспилотных летающих аппаратов, пылесосов-автоматов, в Японии «работают» роботы-полицейские – все эти технологии выполняют свои функции без вмешательства человека. И с каждым годом проникновение таких машин будет только увеличиваться. Одна из нерешаемых задач в вычислительных технологиях – это проблема воссоздания компьютером мышления. Однако можно соединить человеческий мозг с кибернетической, компьютерной системой. Вспомним фильм «Робокоп».

Уже сегодня есть подобные эксперименты, когда протез ноги или руки человека присоединяют к спинному мозгу. Вспомним пример южноафриканского бегуна Оскара Писториуса, с детства лишенного обеих ног, но на соревнованиях обгоняющего абсолютно здоровых конкурентов, благодаря карбоновым протезам. По оценкам экспертов, первый такой «сверх человек», *киберорганизм* появится еще до 2030 года. Он будет ф*изически совершенный, устойчивый к болезням, радиации и экстремальным температурам.* И при этом у него будет мозг человека.

8. Новый статус человека в Интернете. Интернет меняет быт человека. «Всемирная паутина» становится не только площадкой для получения информации и общения, но и инструментом реализации бытовых нужд: таких как совершение покупок, оплата коммунальных услуг и др. Интернет изменил отношение человека с государством. Личное общение, персональное обращения в специальные службы будет минимизировано. Подать документы в вуз, вызвать скорую, написать заявление в полицию, оформить паспорт – все это уже сегодня возможно сделать электронно. Государство и дальше будет вынуждено генерировать услуги через сеть Интернет. Уже сегодня электронный документооборот по всей стране – важнейший приоритет Министерства связи и массовых коммуникаций РФ. Нужно говорить и о новом статусе человека в мире интернет-технологий. Доступ в сеть станет гражданским правом каждого человека, будет свято охраняться и контролироваться законом наряду с прочими гражданскими свободами. Это недалекое будущее. Так, меняется понятие демократии в обществе. Для волеизлияния граждан больше не нужны специальные площадки, трибуны, СМИ. В связи с этим станет и минимум анонимности. Роскоши менять пароли и заводить аккаунты под несуществующими именами, оставлять едкие комментарии под шапкой-невидимкой – скорее всего не станет. Логин/пароль для входа в сеть могут стать средством идентификации личности, а к нему будут привязаны его реальные паспортные данные. Причем, скорее всего это будет не насаждение «сверху», как попытка цензуры и контроля. А желание самого общества, потребность «снизу». Чем больше жизнь в интернете будет реальной, тем больше прозрачности захочется его пользователям. Репутация человека в жизни будет определять его репутацию и в глобальной сети, придуманных биографий не будет. Определив данные человека, сеть сама будет создавать фильтры и пропуски к доступу информацией по возрастным ограничениям, к приватной информации, к различным сервисам в соответствии с платёжеспособностью и даже социальной благонадёжностью.

9. Изменения рынка труда и сферы образования. Активное проникновение сетевых технологий и интернета приведут к изменениям на рынке труда и в сфере образования. Интернет уже превратился в глобальный и ключевой инструмент коммуникации, он все динамичнее превращается из площадки развлечений в площадку труда. Социальные сети, электронная почта, Skype, информационные ресурсы, корпоративные сайты и встроенные в компьютер программы привязывают людей не столько к конкретному офису, сколько к самому компьютеру. А тут уже не важно, откуда ты им пользуешься: с работы, из дома, с кафе или с побережья Индийского океана. Сотрудников, выполняющих свою работу дистанционно, будет все больше. И все больше будет офисов в «кармане», т. е. вирту-

альных предприятий, которые существуют только в Интернете. Людей, получающих образование дистанционно через новые форматы, предоставляемые сетью Интернет – тоже. Для примера, сегодня в Стэндфордском университете лекцию двух профессоров слушают одновременно 25 000 человек!

10. Интернет станет более «зеленым». Сетевые технологии потребляют слишком много энергии, объем его растет, и эксперты сходятся во мнении, что будущая архитектура компьютерных сетей должна быть более энергоэффективной. По данным Национальной лаборатории Лоренса Университета Беркли количество энергии, потребляемой глобальной сетью, в период с 2000 по 2006 год удвоилось(!). Интернет занимает 2 % мирового потребления электроэнергии, что эквивалентно мощности работы 30-ти атомных электростанций – 30 млрд Вт. Тенденция к «озеленению» или «экологизации» сети Интернет будет ускоряться по мере роста цен на энергоносители.

11. Кибероружие и кибервойны. У развития интернет-технологий и возможностей компьютерных сетей есть и другая сторона медали. Начиная от киберпреступлений, связанных с увеличением в интернете электронной коммерции, до кибервойн. Киберпространство уже официально признано пятым «полем боя» (таким же как суша, море, воздушное пространство и космос). Военно-морские силы США в 2010 году даже создали кибервойска CYBERFOR, которые находятся в непосредственном подчинении у командования ВМС США. Сегодня под вирусные атаки хакеров попадают не только ПК рядовых пользователей, но и промышленные системы, управляющие автоматизированными производственными процессами. Вредоносный червь может быть использован в качестве шпионажа, а так же диверсий электростанций, аэропортов и других жизнеобеспечивающих предприятий. Так, в 2010 году компьютерный червь Stuxnet поразил ядерные объекты Ирана, отбросив атомную программу этой страны на два года назад. Применение вредоносной программы оказалось по эффективности сравнимо с полноценной военной операцией, но при отсутствии жертв среди людей. Уникальность этой программы заключалась в том, что впервые в истории кибератак вирус физически разрушил инфраструктуру. Совсем недавно, 27 марта этого года произошла крупнейшая хакерская атака в истории, которая даже снизила скорость передачи данных во всем Интернете. Мишенью атаки стала европейская компания Spamhaus, занимающаяся противодействием рассылке спама. Мощность DDoS-атак составила 300 Гбит/сек, при том что мощности в 50 Гбит/сек хватает для того, чтобы вывести из строя инфраструктуру крупной финансовой организации. Проблема национальной безопасности – один из важнейших вопросов, стоящих на повестке дня в развитых странах. Нынешняя архитектура компьютерных сетей такую безопасность обеспечить не может. Поэтому индустрия антивирусов/web-защиты и разработки новых технологий по обеспечению безопасности будет расти с каждым годом

12. Выход интернета и сетевых технологий в космос. Сегодня сеть Интернет носит планетарный масштаб. На повестке дня – межпланетное пространство, космический Интернет.

Международная космическая станция подключена к сети Интернет, что значительно ускоряет процессы работы и взаимодействия станции с Землей. Но обычное установление связи при помощи оптико-волоконного или простого кабеля, которое очень эффективно в земных условиях, невозможно в космосе. В частности из-за того, что невозможно применять в межпланетном пространстве обычный протокол TCP/IP (протокол – особый «язык» компьютерных сетей для «общения» друг с другом).

Исследовательские работы по созданию нового протокола, благодаря которому Интернет мог бы функционировать и на лунных станциях, и на Марсе, ведутся. Так, один из подобных протоколов называется Disruption Tolerant Networking (DTN). Компьютерные сети с этим протоколом уже были применены для связи МКС с Землей, в частности по каналам связи были отправлены фотографии солей, которые были получены в состоянии невесомости. Но эксперименты в этой сфере продолжаются.

Интернет за два с лишним десятка лет его развития практически не менялся концептуально и архитектурно. С одной стороны, внедрялись новые технологии передачи данных, с другой – создавались новые сервисы, но основная концепция сети, архитектура компьютерных сетей остаются на уровне 80-х годов прошлого столетия. Перемены не только давно назрели, но и жизненно необходимы. На основе старой архитектуры невозможны инновации. Компьютерные сети уже сегодня работают на пределе своих возможностей, и ту нагрузку, которую предстоит испытать сетям при таком активном росте, они могут просто не выдержать. Развитие и внедрение всех перечисленных тенденций возможно только после внедрения новой, более гибкой архитектуры компьютерных сетей. Во всем научном ИТ-мире это вопрос № 1.

Самая перспективная на сегодня технология/архитектура компьютерных сетей, которая способна вывести из кризиса, – это **технология программно-конфигурируемых сетей (softwere definednetwork).** В 2007 году сотрудниками университета Стэнфорда и Беркли был разработан новый «язык» общения компьютерных сетей – **протокол OpenFlow** и новый алгоритм работы компьютерных сетей – ПКС технология**.** Ее основная ценность в том, что она позволяет уйти от «ручного» управления сетью. В современных сетях функции управления и передачи данных совмещены, что делает контроль и управление очень сложным. ПКС-архитектура разделяет процесс управления и процесс передачи данных. Что открывает колоссальные возможности для развития интернет-технологий, так как ПКС не в чем нас не ограничивает, выводя на первый план программное обеспечение. В России изучением ПКС занимается Центр прикладных исследований компьютерных сетей.

6. Основные понятия информационной безопасности

Прежде чем говорить об обеспечении безопасности персональных данных, необходимо определить, что же такое *информационная безопасность*. Термин «*информационная безопасность*» может иметь различный смысл и трактовку в зависимости от контекста. В данном курсе под **информационной безопасно-**

стью мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб субъектам информационных отношений*, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

ГОСТ «*Защита информации*. Основные термины и определения» вводит понятие **информационной безопасности** как состояние защищенности информации, при котором обеспечены ее *конфиденциальность*, доступность и *целостность*.

- **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
- **Целостность** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- **Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Угрозы информационной безопасности – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. **Атакой** называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, – **злоумышленником**. Потенциальные злоумышленники называются *источниками угрозы*.

Угроза является следствием наличия **уязвимых мест или уязвимостей** в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ.

Угрозы можно классифицировать по нескольким критериям:

- по *свойствам информации* (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, *поддерживающая инфраструктура*);
- по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется *комплексный подход*. Выделяют следующие уровни защиты информации:

1) законодательный – законы, нормативные акты и прочие документы РФ и международного сообщества;
2) административный – комплекс мер, предпринимаемых локально руководством организации;
3) процедурный уровень – меры безопасности, реализуемые людьми;
4) *программно-технический уровень* – непосредственно средства защиты информации.

Законодательный уровень является основой для построения системы защиты информации, так как дает базовые понятия *предметной области* и определяет меру наказания для потенциальных злоумышленников. Этот уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) *отношение* к людям, нарушающим информационную *безопасность*.

1.2. ФЗ «Об информации, информационных технологиях и о защите информации»

В российском законодательстве базовым законом в области защиты информации является ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года номер 149-ФЗ. Поэтому основные понятия и решения, закрепленные в законе, требуют пристального рассмотрения.

Закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Закон дает основные определения в области защиты информации. Приведем некоторые из них:

- **информация** – сведения (сообщения, данные) независимо от формы их представления;
- **информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- **информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- **обладатель информации** – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
- **оператор информационной системы** – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.
- **конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

В статье 4 Закона сформулированы принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Вся *информация* делится на **общедоступную** и ограниченного **доступа**. К общедоступной информации относятся общеизвестные сведения и иная *информация*, *доступ* к которой не ограничен. В законе, определяется *информация*, к которой нельзя ограничить *доступ*, например, *информация* об окружающей среде или деятельности государственных органов. Оговаривается также, что *ограничение доступа* к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, *доступ* к которой ограничен федеральными законами.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Закон выделяет 4 категории информации в зависимости от порядка ее предоставления или распространения:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Закон устанавливает равнозначность электронного сообщения, подписанного электронной цифровой подписью или иным аналогом собственноручной подписи, и документа, подписанного собственноручно.

Дается следующее *определение* защите информации - представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

Таким образом, ФЗ «Об информации, информационных технологиях и о защите информации» создает правовую основу информационного обмена в РФ и определяет *права* и обязанности его субъектов.

7. Технологии обеспечения безопасности в локальных сетях

Основы сетевой безопасности. Сеть как объект защиты

Преступность в сфере информационных технологий (киберпреступность) – явление, получившее глобальное распространение буквально в течение нескольких лет. Эффективная борьба с киберпреступлениями требует международного сотрудничества на государственном уровне.

Первые вирусы для IBM PC-совместимых компьютеров появились в 90-х годах XX века. С тех пор характер угроз стал принципиально другим, отразив изменения в технологии, внедрение компьютеров во все новые сферы жизни и рост числа пользователей. В любой сфере человеческой деятельности каждое новое поколение принимает эстафету у предыдущего, учась на его достижениях. Это относится и к создателям вредоносного кода: несколько поколений вирусописателей полностью изменили ситуацию с угрозами информационной безопасности.

Чуть более десятка лет назад вирусы и другие вредоносные программы использовались для осуществления одиночных актов компьютерного вандализма и антисоциального самовыражения с применением сложных технических средств. Большинство вирусов ограничивались заражением компьютерных дисков и программ. А ущерб в основном сводился к потере данных, поскольку вирусы стирали или портили данные на диске.

Аль Капоне от IT. Едва ли не первый громкий взлом совершил еще в 1983 году один из самых известных в будущем киберпреступников Кевин Митник, то-

гда еще простой американский студент. Используя университетский компьютер, он проник в компьютерную сеть ARPANet (предшественницу Internet) и сумел войти в компьютеры Пентагона. Он получил доступ ко всем файлам министерства обороны США. Митника арестовали прямо на территории университета. Он был осужден на полгода в исправительном центре для молодежи.

Теперь все иначе. Сегодня киберпреступность – масштабная проблема, а вредоносные программы пишутся с целью незаконного получения денег. Развитие интернета стало одним из ключевых факторов, определивших эти перемены. Компании и отдельные пользователи все больше финансовых операций проводят через Интернет. Киберпреступники осознали, какие огромные возможности для «зарабатывания» денег с помощью вредоносного кода появились в последнее время, и многие из нынешних вредоносных программ написаны по заказу или с целью последующей продажи другим преступникам.

Для обеспечения информационной безопасности разработано множество методов и средств, но одним из ее важнейших аспектов является определение, анализ и классификация возможных угроз. Их перечень, оценки вероятностей реализации, а также модель нарушителя служат основой для проведения анализа риска и формулирования требований к системе защиты сети предприятия.

Сеть как объект защиты

Большинство современных автоматизированных систем обработки информации представляют собой распределенные системы, построенные на стандартных сетевых архитектурах и использующие типовые наборы сетевых сервисов и прикладного программного обеспечения. Корпоративные сети «наследуют» все «традиционные» для локальных вычислительных систем способы несанкционированного вмешательства. Кроме того, для них характерны и специфические каналы проникновения и несанкционированного доступа к информации, обусловленные использованием сетевых технологий.

Перечислим основные особенности распределенных вычислительных систем:

- территориальная удаленность компонентов системы и наличие интенсивного обмена информацией между ними;
- широкий спектр используемых способов представления, хранения и передачи информации;
- интеграция данных различного назначения, принадлежащих различным субъектам, в рамках единых баз данных и, наоборот, размещение необходимых некоторым субъектам данных в различных удаленных узлах сети;
- абстрагирование владельцев данных от физических структур и места размещения данных;
- использование режимов распределенной обработки данных;
- участие в процессе автоматизированной обработки информации большого количества пользователей и персонала различных категорий;
- непосредственный и одновременный доступ к ресурсам большого числа пользователей;
- разнородность используемых средств вычислительной техники и программного обеспечения;

Уязвимость компонентов распределенных АС

В общем случае ЛВС состоит из следующих основных структурно-функциональных элементов:

- рабочих станций;
- серверов;
- межсетевых коммуникационных узлов (шлюзов, мостов, маршрутизаторов);
- каналов связи.

Рабочие станции считаются наиболее доступными компонентами сетей и именно с них могут быть предприняты наиболее многочисленные попытки совершения несанкционированных действий.

С рабочих станций осуществляется управление процессами обработки информации, запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы обработки.

На видеомониторы и печатающие устройства рабочих станций выводится информация при работе пользователей, выполняющих различные функции и имеющих разные полномочия по доступу к ресурсам системы.

Серверы и **коммуникационное оборудование** нуждаются в особой защите, поскольку наиболее привлекательны с точки зрения злоумышленников. Первые – как концентраторы больших объемов информации, вторые – как элементы, в которых осуществляется преобразование (возможно через открытую, нешифрованную форму представления) данных при согласовании протоколов обмена в различных участках сети.

Каналы связи, в силу большой пространственной протяженности через неконтролируемую или слабо контролируемую территорию, представляют возможность как прямого подключения к ним, так и вмешательства в процесс передачи данных.

Угрозы безопасности информации

Под угрозой (вообще) обычно понимают потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам. Угрозой интересам субъектов информационных отношений будем называть такое событие, процесс или явление, которое посредством воздействия на информацию или другие компоненты АС может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.

В силу приведенных ранее особенностей современных АС, существует значительное число различных видов угроз.

Виды угроз информационной безопасности

Основными видами угроз безопасности сети являются:

- стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т. п.);
- сбои и отказы оборудования (технических средств) АС;
- последствия ошибок в проектировании и разработке компонентов АС (аппаратных средств, технологии обработки информации, программ, структур данных и т. п.);
- ошибки эксплуатации (пользователей, операторов и другого персонала);

- преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т. п.).

Все виды могут быть классифицированы по разным признакам, что позволяет более эффективно использовать средства защиты информации.

Классификация угроз информационной безопасности

Все множество потенциальных угроз по природе их возникновения разделяется на два класса: естественные (объективные) и искусственные (субъективные).

Естественные угрозы – это объективные, не зависимые от человека, факторы, способные нарушить безопасность сети. Угрозы этого типа относят к форс-мажорным.

Искусственные угрозы, напротив, вызваны преднамеренной (умышленные угрозы) или непреднамеренной (неумышленные) деятельностью человека:

- неумышленные угрозы – связаны с ошибками в проектировании и развертывании сети, ошибками в программном обеспечении, в действиях персонала и т. п.;
- умышленные угрозы – основаны на корыстных устремлениях людей (злоумышленников).

Источники угроз по отношению к ЛВС разделяются на:

- внутренние – структурные элементы самой сети, включая аппаратное, программное обеспечение и обслуживающий персонал;
- внешние – все прочие.

Основные непреднамеренные искусственные угрозы

УК РФ. Глава 28. Преступления в сфере компьютерной информации

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, – наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок до четырех лет.

Основные непреднамеренные искусственные угрозы АС (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

1) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т. п.);

2) неправомерное включение оборудования или изменение режимов работы устройств и программ;

3) неумышленная порча носителей информации;

4) запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацик-

ливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т. п.);

5) нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

6) заражение компьютера вирусами;

7) неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;

8) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т. п.);

9) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;

10) игнорирование организационных ограничений (установленных правил) при ранге в системе;

11) вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т. п.);

12) некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;

13) пересылка данных по ошибочному адресу абонента (устройства);

14) ввод ошибочных данных;

15) неумышленное повреждение каналов связи.

Основные преднамеренные искусственные угрозы

УК РФ. Глава 28. Преступления в сфере компьютерной информации

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Основные возможные пути умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

1) физическое разрушение системы или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы;

2) вывод из строя подсистем обеспечения функционирования сети;

3) дезорганизация функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т. п.);

4) внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);

5) вербовка (путем подкупа, шантажа и т. п.) персонала или отдельных пользователей, имеющих определенные полномочия;

6) применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;

7) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т. п.);

8) перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

9) хищение носителей информации;

10) несанкционированное копирование носителей информации;

11) хищение производственных отходов (распечаток, записей, списанных носителей информации и т. п.);

12) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

13) чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме используя недостатки мультизадачных операционных систем и систем программирования;

14) незаконное получение паролей и других реквизитов разграничения доступа с дальнейшим их использованием;

15) несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т. п.;

16) вскрытие криптографических шифров;

17) внедрение аппаратных и программных "закладок" и "вирусов";

18) незаконное подключение к линиям связи с целью работы "между строк", с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;

19) незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и

успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

УК РФ. Глава 28. Преступления в сфере компьютерной информации

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами – наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказываются лишением свободы на срок от трех до семи лет.

Следует заметить, что чаще всего для достижения поставленной цели злоумышленник использует не один, а несколько перечисленных выше путей.

Классификация каналов проникновения в систему и утечки информации

Все каналы проникновения в систему и утечки информации разделяют на прямые и косвенные. Под косвенными понимают такие каналы, использование которых не требует проникновения в помещения, где расположены компоненты системы. Для использования прямых каналов такое проникновение необходимо. Прямые каналы могут использоваться без внесения изменений и компоненты системы или с изменениями компонентов.

По типу основного средства, используемого для реализации угрозы все возможные каналы можно условно разделить на три группы, где таковыми средствами являются: человек, программа или аппаратура.

По способу получения информации потенциальные каналы утечки можно разделить на:

- физический;
- электромагнитный (перехват излучений);
- информационный (программно-математический).

При контактном НСД (физическом, программно-математическом) возможные угрозы информации реализуются путем доступа к элементам АС, к носителям информации, к самой вводимой и выводимой информации (и результатам), к программному обеспечению (в том числе к операционным системам), а также путем подключения к линиям связи и перехвата сетевого трафика.

При бесконтактном доступе (например, по электромагнитному каналу) возможные угрозы информации реализуются перехватом излучений аппаратуры АС.

Неформальная модель киберпреступника

Преступления, в том числе и компьютерные, совершаются людьми. Пользователи системы и ее персонал, с одной стороны, являются составной частью, необходимым элементом АС. С другой стороны, они же являются основной причиной и движущей силой нарушений и преступлений. В этом смысле вопросы безо-

пасности автоматизированных систем суть вопросы человеческих отношений и человеческого поведения.

Нарушитель – лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового и использующее для этого различные возможности, методы и средства. Злоумышленником будем называть нарушителя, намеренно идущего на нарушение из корыстных побуждений.

Неформальная модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т.п. Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы. Исследовав причины нарушений, можно либо повлиять на сами эти причины (насколько это возможно), либо точнее определить требования к системе защиты от данного вида нарушений или преступлений.

В каждом конкретном случае, исходя из конкретной технологии обработки информации, может быть определена модель нарушителя, которая должна быть адекватна реальному нарушителю для данной АС. При разработке модели нарушителя определяются:

- предположения о категориях лиц, к которым может принадлежать нарушитель;
- предположения о мотивах действий нарушителя (преследуемых целях);
- предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);
- ограничения и предположения о характере возможных действий нарушителей.

По отношению к АС нарушители могут быть внутренними (из числа персонала системы) или внешними (посторонними лицами). Внутренним нарушителем может быть лицо из следующих категорий персонала:

- пользователи (операторы) системы;
- персонал, обслуживающий технические средства (инженеры, техники),
- сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты);
- технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты АС);
- сотрудники службы безопасности АС;
- руководители различных уровней должностной иерархии.

Посторонние лица, которые могут быть нарушителями:

- клиенты (представители организаций, граждане);
- посетители (приглашенные по какому-либо поводу);
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т. п.);
- представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;

- лица, случайно или умышленно нарушившие пропускной режим (без цели нарушить безопасность АС);
- любые лица за пределами контролируемой территории.

Можно выделить три основных мотива нарушений: *безответственность*, *самоутверждение* и *корыстный интерес*.

При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные тем не менее со злым умыслом. Такого рода нарушения информационной безопасности особенно характерны для домашних пользователей, которые по некомпетентности или небрежности теряют контроль над приватной информацией. Существенно снизить этот риск позволяет использование специализировнного ПО, такого как антивирусы, персональные файрволлы и системы контроля трафика.

Некоторые пользователи считают получение доступа к системным наборам данных крупным успехом, затевая своего рода игру «пользователь против системы» ради самоутверждения либо в собственных глазах, либо в глазах коллег.

Нарушение безопасности АС может быть вызвано и корыстным интересом пользователя системы. В этом случае он будет целенаправленно пытаться преодолеть систему защиты для доступа к хранимой, передаваемой и обрабатываемой в АС информации. Даже если АС имеет средства, делающие такое проникновение чрезвычайно сложным, полностью защитить ее от проникновения практически невозможно.

Всех нарушителей можно классифицировать следующим образом.

По уровню знаний об АС:

- знает функциональные особенности АС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами;
- обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;
- обладает высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;
- знает структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.

Хакер – высококвалифицированный ИТ-специалист, человек, который понимает самые основы работы компьютерных систем. В числе хакеров такие представители ИТ-индустрии, как Ричард М. Столлман, Линус Торвальдс, Деннис Ритчи, Кен Томпсон, Цутому Шимамура, Стив Возняк.

Средства массовой промывки мозгов неправильно называют хакерами компьютерных преступников-крэкеров (от англ. to crack – ломать), взломщиков вычислительных систем.

По уровню возможностей (используемым методам и средствам):

- применяющий чисто агентурные методы получения сведений;
- применяющий пассивные средства (технические средства перехвата без модификации компонентов системы);

- использующий только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные магнитные носители информации, которые могут быть скрытно пронесены через посты охраны;
- применяющий методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

По времени действия:

- в процессе функционирования АС (во время работы компонентов системы);
- в период простоя компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерывов для обслуживания и ремонта и т. п.);
- как в процессе функционирования АС, так и в период простоя компонентов системы.

По месту действия:

- без доступа на контролируемую территорию организации;
- с контролируемой территории без доступа в здания и сооружения;
- внутри помещений, но без доступа к техническим средствам АС;
- с рабочих мест конечных пользователей (операторов) АС;
- с доступом в зону данных (баз данных, архивов и т. п.):
- с доступом в зону управления средствами обеспечения безопасности АС.

Могут учитываться следующие ограничения и предположения о характере действий возможных нарушителей:

- работа по подбору кадров и специальные мероприятия затрудняют возможность создания коалиций нарушителей, т. е. объединения (сговора) и целенаправленных действий по преодолению подсистемы защиты двух и более нарушителей;
- нарушитель, планируя попытки НСД, скрывает свои несанкционированные действия от других сотрудников;
- НСД может быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки информации и т. д.

Определение конкретных значений характеристик возможных нарушителей в значительной степени субъективно. Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена перечислением нескольких вариантов его облика. Каждый вид нарушителя должен быть охарактеризован значениями характеристик, приведенных выше.

Киберпреступность: модные тренды

Специфика сетей, с точки зрения их уязвимости, связана в основном с наличием интенсивного информационного взаимодействия между территориально разнесенными и разнородными элементами.

Уязвимыми являются буквально все основные структурно-функциональные элементы распределенных АС: рабочие станции, серверы, межсетевые мосты (шлюзы, центры коммутации), каналы связи.

Имеется широчайший спектр вариантов путей преднамеренного или случайного несанкционированного доступа к данным и вмешательства в процессы обработки и обмена информацией.

Все это говорит о том, что киберпреступность никуда не исчезнет. Киберпреступность – не только побочный продукт эпохи Интернета, но и часть общего криминального ландшафта. Если что-то можно использовать, то кто-то обязательно найдет возможность использовать это во зло. Компьютерные сети – не исключение. Развитие информационных технологий и расширение сетевых услуг (см. перспективы развития сетей) влечет за собой не только увеличение числа подключенных пользователей, но и совершенствование методов и средств, применяемых киберпреступниками.

Так, эксперты компании «McAfee Labs» среди основных тенденций в сфере киберпреступлений еще в начале 2011 года выделили следующие:

- Социальные сети. Они станут одной из основных целей для киберугроз. Причем объектом атак будут становиться не только сами сайты сетей, но и приложения для них, разработанные третьими сторонами.
- Внедрение HTML5. Этот язык представляет пользователям возможности перехода от настольных приложений к онлайн-приложениям, а мошенникам – для создания вредоносного ПО, распространяемого через веб-сайты.
- Вредоносное ПО будет усложняться, оно будет становиться все более «интеллектуальным», моделирующим поведенческие факторы онлайн-пользователей и использующим психологические методы.
- Все большее внимание злоумышленников будет обращено на пользователей мобильных телефонов и смартфонов.
- Поменяется также и инфраструктура ботнетов. Если сейчас они имеют в основном централизованную архитектуру, то в ближайшем будущем они станут пиринговыми (p2p, peer-to-peer – аналог торрент-сетей).

Рост объемов киберпреступности привлекает внимание государства, и соответственно, является объектом законодательных инициатив. Однако теперь уже ясно, что преступность в сфере информационных технологий – явление глобальное. Следовательно, для эффективной борьбы с киберпреступностью необходимо сотрудничество на международном уровне, чтобы обеспечить преследование киберпреступников, невзирая на геополитические границы.

Европейская конвенция о киберпреступности

Одно из наиболее серьезных ограничений национального законодательства о компьютерных преступлениях состоит в том, что оно не позволяет эффективно бороться с глобальным явлением киберпреступности. Европейская конвенция о киберпреступности, разработанная с целью создания международной структуры для борьбы с киберпреступлениями, была принята Комитетом министров Совета Европы в ноябре 2001 года, а вступила в силу 1 июля 2004 года.

Конвенция охватывает широкий круг вопросов, в том числе все аспекты киберпреступности, включая незаконный доступ к компьютерным системам и перехват данных, воздействие на данные, воздействие на работу системы, противозаконное использование устройств, подлог и мошенничество с использованием компьютерных технологий, правонарушения, связанные с детской порнографией, и правонарушения, связанные с авторским правом и смежными правами. При подготовке конвенции также преследовались цели формирования общей правоохранительной системы для борьбы с киберпреступностью и создания условий для обмена информацией между всеми странами, подписавшими конвенцию.

8. Обеспечение безопасности сетей на базе сетевых операционных систем

Причины возникновения уязвимостей ОС

- ошибки проектирования (компонент ядра, подсистем)
- ошибки реализации (кода)
- ошибки эксплуатации (неправильная настройка, неиспользуемые компоненты, слабые пароли)

Источники информации о новых уязвимостях:

- www.cert.org – координационный центр CERT/CC
- www.iss.net/xforce - база данных компании ISS

А также:

- www.sans.org
- www.securityfocus, co,
- www.ciac.org/ciac/

Примеры уязвимостей.

- nt-getadmm-present

Описание: проблема одной из функций ядра ОС Windows NT, позволяющая злоумышленнику повысить привилегии обычного пользователя до привилегий администратора

Источник возникновения: *ошибки реализации*

- explorer-relative-path-name

Описание: реестре Windows NT/2000 указан относительный путь к файлу explorer.exe (Windows shell) вместо абсолютного пути.

Источник возникновения: *ошибки реализации*

Ошибки проектирования:

- Отсутствие ограничений на количество создаваемых объектов
- Особенности шифрования (хэширования) и хранения паролей

…

Ошибки обслуживания:

- идентификация и аутентификация,
- разграничение доступа (и авторизация),
- регистрация событий (аудит),
- контроль целостности,
- затирание остаточной информации,

– криптографические механизмы.

Проблемы обеспечения безопасности ОС

Большинство программных средств защиты информации являются прикладными программами. Для их выполнения требуется поддержка ОС. Окружение, в котором функционирует ОС, называется *доверенной вычислительной базой* (ДВБ). ДВБ включает в себя полный набор элементов, обеспечивающих информационную безопасность: ОС, программы, сетевое оборудование, средства физической защиты и даже организационные процедуры. Краеугольным камнем этой пирамиды является защищенная ОС.

Угрозы безопасности ОС

Организация эффективной и надежной защиты ОС невозможна без предварительного анализа возможных угроз ее безопасности. Угрозы безопасности ОС существенно зависят от условий эксплуатации системы, от того, какая информация хранится и обрабатывается в системе, и т. д. Например, если ОС используется для организации электронного документооборота, наиболее опасны угрозы, связанные с несанкционированным доступом (НСД) к файлам. Если же ОС используется как платформа провайдера интернет-услуг, очень опасны атаки на сетевое программное обеспечение ОС.

Угрозы безопасности ОС можно классифицировать по различным аспектам их реализации [56].

1. По *цели атаки.*

• несанкционированное чтение информации;

• несанкционированное изменение информации;

• несанкционированное уничтожение информации;

• полное или частичное разрушение ОС.

2. По *принципу воздействия на операционную систему:*

• использование известных (легальных) каналов получения информации; например угроза несанкционированного чтения файла, доступ пользователей к которому определен некорректно, т. е. разрешен доступ пользователю, которому согласно политике безопасности доступ должен быть запрещен;

• использование скрытых каналов получения информации; например угроза использования злоумышленником недокументированных возможностей ОС;

• создание новых каналов получения информации с помощью программных закладок.

3. По *типу используемой злоумышленником уязвимости защиты:*

• неадекватная политика безопасности, в том числе и ошибки администратора системы;

• ошибки и недокументированные возможности программного обеспечения ОС, в том числе и так называемые *люки* – случайно или преднамеренно встроенные в систему «служебные входы», позволяющие обходить систему защиты;

• ранее внедренная программная закладка.

4. По *характеру воздействия на операционную систему:*

• активное воздействие – несанкционированные действия злоумышленника в системе;

• пассивное воздействие – несанкционированное наблюдение злоумышленника за процессами, происходящими в системе.

Угрозы безопасности ОС можно также классифицировать по таким признакам, как: способ действий злоумышленника, используемые средства атаки, объект атаки, способ воздействия на объект атаки, состояние атакуемого объекта ОС на момент атаки.

ОС может подвергнуться следующим типичным атакам:

• *сканированию файловой системы*. Злоумышленник просматривает файловую систему компьютера и пытается прочесть (или скопировать) все файлы подряд. Рано или поздно обнаруживается хотя бы одна ошибка администратора. В результате злоумышленник получает доступ к информации, который должен быть ему запрещен;

• *подбору пароля*. Существуют несколько методов подбора паролей пользователей:

— тотальный перебор;

— тотальный перебор, оптимизированный по статистике встречаемости символов или с помощью словарей;

— подбор пароля с использованием знаний о пользователе (его имени, фамилии, даты рождения, номера телефона и т. д.);

• *краже ключевой информации.* Злоумышленник может подсмотреть пароль, набираемый пользователем, или восстановить набираемый пользователем пароль по движениям его рук на клавиатуре. Носитель с ключевой информацией (смарт-карта, Touch Memory и т. д.) может быть просто украден;

• *сборке мусора*. Во многих ОС информация, уничтоженная пользователем, не уничтожается физически, а помечается как уничтоженная (так называемый *мусор).*Злоумышленник восстанавливает эту информацию, просматривает ее и копирует интересующие его фрагменты;

• *превышению полномочий*. Злоумышленник, используя ошибки в программном обеспечении ОС или политике безопасности, получает полномочия, превышающие те, которые ему предоставлены в соответствии с политикой безопасности. Обычно это достигается путем запуска программы от имени другого пользователя;

• *программным закладкам*. Программные закладки, внедряемые в ОС, не имеют существенных отличий от других классов программных закладок;

• *жадным программам* – это программы, преднамеренно захватывающие значительную часть ресурсов компьютера, в результате чего другие программы не могут выполняться или выполняются крайне медленно. Запуск жадной программы может привести к краху ОС [56].

9. Обеспечение безопасности межсетевого взаимодействия

Обеспечение безопасного межсетевого взаимодействия в ИСПДн на примере использованием программного комплекса UserGate Proxy&Firewall 5.2.F

Одним из обязательных методов защиты от несанкционированного доступа (НСД) информационных систем обрабатывающих конфиденциальную информацию или персональные данные (ИСПДн), имеющих доступ в Интернет, является обеспечение безопасного межсетевого взаимодействия. Безопасное межсетевое взаимодействие достигается применением средств межсетевого экранирования, обеспечивающих выполнение следующих функций:

- фильтрацию на сетевом уровне независимо для каждого сетевого пакета (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
- фильтрацию с учетом любых значимых полей сетевых пакетов;
- регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);
- идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
- регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
- регистрацию запуска программ и процессов (заданий, задач);
- контроль целостности своей программной и информационной части;
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
- регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

Используемые для защиты ИСПДн межсетевые экраны помимо соответствия перечисленным требованиям должны пройти, установленным порядком, процедуру сертификации на соответствие требованиям безопасности.

В качестве комплексного решения для межсетевого экранирования ИСПДн, предлагается использовать UserGate Proxy&Firewall 5.2.F. Кроме организации безопасного доступа в Интернет, UserGate позволяет обеспечивать:

- дополнительную защиту от сетевых атак и других типов вторжений, блокируя трафик по определенным портам (TCP, UDP или любой другой IP-протокол);
- создание различных наборов правил для управления внешним и внутренним трафиком;
- комплексную антивирусную защиту. В целях качественной проверки трафика на предмет наличия вредоносного ПО, в UserGate могут быть включены два антивирусных модуля – Антивирус Касперского и Panda Antivirus. При этом обеспечивается двойная антивирусная проверка трафика по протоколам HTTP, FTP, SMTP и POP3.
- полный контроль над использованием Интернет-трафика в компании. На основе данных статистики руководители могут определять политику доступа в Интернет в компании, которая затем реализуется с помощью гибкой системы правил управления трафиком в UserGate;
- простое администрирование сетевыми ресурсами. Встроенный DHCP-сервер автоматизирует процесс выдачи IP-адресов устройствам в локальной сети. Если компьютер с UserGate подключен к нескольким локальным сетям, сервер UserGate можно настроить как маршрутизатор (router), обеспечив прозрачную, двунаправленную связь между локальными сетями. Публикация ресурсов позволяет предоставить доступ к внутренним ресурсам компании, например к Web, FTP, VPN или к почтовому серверу;
- удаленное администрирование по локальной сети или через Интернет с любого компьютера, на котором установлена Консоль Администрирования UserGate и др.

UserGate Proxy&Firewall 5.2.F сертифицирован на соответствие требованиям руководящих документов ФСТЭК (Гостехкомиссии) России:

- «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» – по ОУД2;
- «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации» – по 4 классу защищенности;
- «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» – по 4 уровню контроля.

UserGate Proxy & Firewall 5.2.F может использоваться для защиты:

- конфиденциальной информации в автоматизированных системах до класса защищенности 1Г включительно;
- персональных данных в информационных системах персональных данных до 1-го класса включительно.

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ДОКУМЕНТОВ ФСТЭК РОССИИ

	Основные механизмы защиты UserGate Proxy&Firewall 5.2.F	Требования документов ФСТЭК России к межсетевому экранированию				
		РД АС	Положение о методах и способах защиты информации в ИСПДн			
		1Г	К4	К3	К2	К1
1.	Фильтрация на сетевом уровне для каждого сетевого пакета	+	+	+	+	+
2.	Фильтрация пакетов служебных протоколов	+	+	+	+	+
3.	Фильтрация с учетом выходного и выходного сетевого интерфейса	+	0	0	+	+
4.	Фильтрация с учетом полей сетевых пакетов	+	0	0	+	+
5.	Фильтрация на транспортном уровне запросов на установление виртуальных соединений	0	0	0	0	+
6.	Фильтрация на прикладном уровне запросов к прикладным сервисам	0	0	0	0	+
7.	Идентификация и аутентификация администраторов при локальном доступе	+	+	+	+	+
8.	Предотвращение доступа неидентифицированного пользователя	0	0	0	0	+
9.	Аутентификация входящих и исходящих запросов методами устойчивыми к пассивному и (или) активному прослушиванию	0	0	0	0	±[1]
10.	Регистрация входа (выхода)	+	+	+	+	+
11.	Регистрация и учет фильтруемых пакетов	+	0	0	+	+
12.	Регистрация запуска программ и процессов	+	0	0	+	+
13.	Регистрация действий администратора	0	0	0	0	+
14.	Регистрация виртуальных соединений	0	0	0	0	+
15.	Возможность дистанционного управления	0	0	0	0	+
16.	Контроль целостности	+	+	+	+	+
17.	Контроль целостности по контрольным суммам	0	0	0	0	+
18.	Сигнализация попыток нарушения правил фильтрации	0	+	+	+	+
19.	Восстановление свойств после сбоев и отказов	+	+	+	+	+
20.	Регламентное тестирование	+	+	+	+	+

+ – требования выполняются

0 – не предъявляются требования

1 – требование выполняется при настройке запрета на удаленное администрирование либо при использовании наложенных сертифицированных средств аутентификации, для удаленной авторизации на сервере UserGate;

Типовой вариант использования программного комплекса UserGate Proxy&Firewall 5.2.F подразумевает сегментирование сети, имеющей доступ в Интернет, на различные зоны сетевой безопасности (каждая с определенным уровнем доступа и контроля) в соответствии с корпоративной политикой доступа к информационным ресурсам и организацию фильтрации сетевого трафика по задаваемым правилам (фильтрам). Ниже представлен вариант системы фильтров, наиболее обще отражающей спектр основных задач обеспечения контролируемой защиты «периметра» корпоративной сети (см. рисунок):

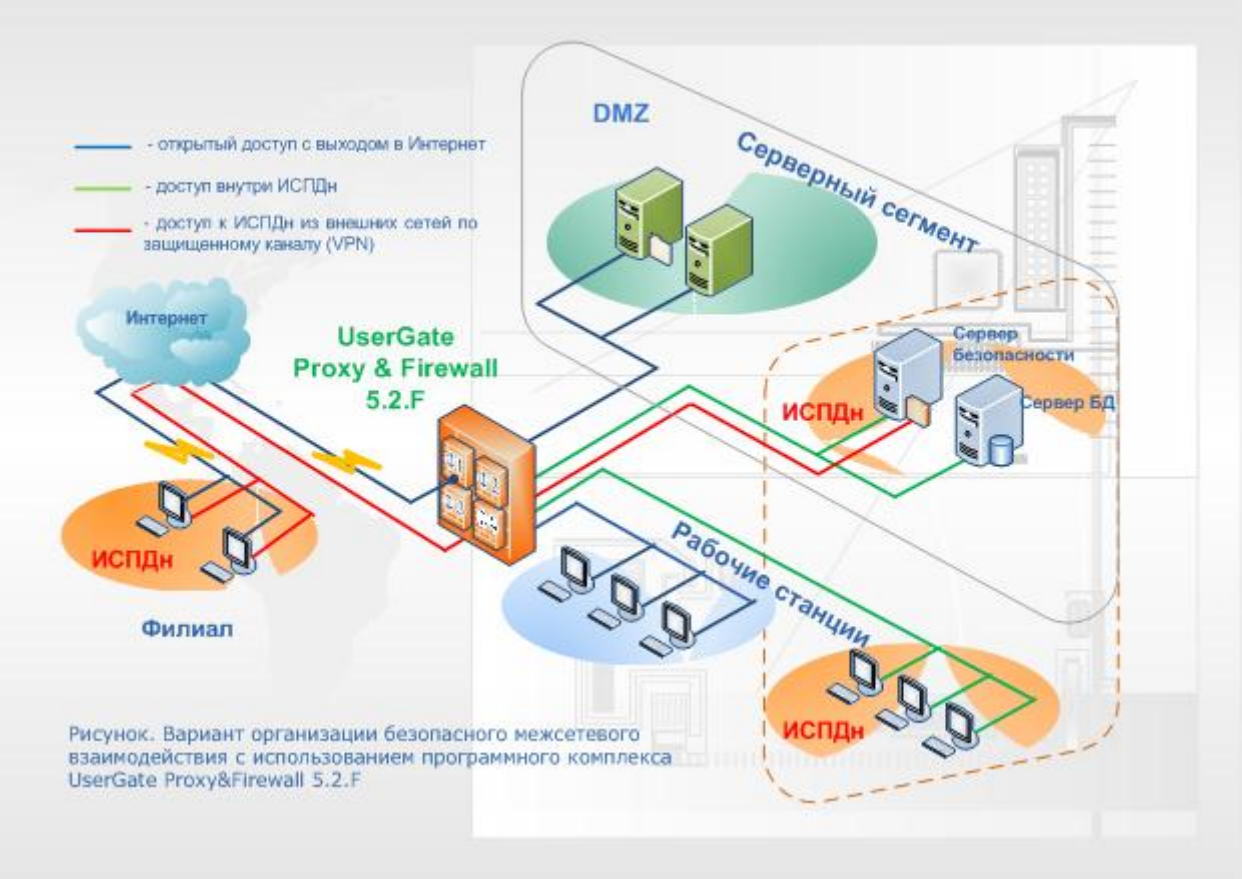


Рисунок. Вариант организации безопасного межсетевого взаимодействия с использованием программного комплекса UserGate Proxy&Firewall 5.2.F

- Внешние пользователи имеют доступ в демилитаризованную зону (DMZ), не входящую в состав ИСПДн, по определенному набору коммуникационных протоколов (Ф1);
- Доступ к ИСПДн из удаленного офиса и внешних сетей производится по защищенному каналу (VPN) (Ф 2);
- Обмен данными пользователей ИСПДн и их доступ к серверному сегменту (базе данных, серверу безопасности и пр.) организован по строго ограниченному набору протоколов и правил (Ф3);
- Пользователи корпоративной сети для доступа в открытую сеть Интернет используют proxy-сервисы межсетевого экрана, (фильтр 4).

10. Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот.

Технология конфиденциального документооборота

Понятие документооборота. Основополагающее единство движения документов и информации. Документооборот и жизненный цикл документа. Роль и место документооборота в процессе управления организационными структурами и производственными процессами. Информационно-документационное обеспечение деятельности, работы. Требования, предъявляемые к документообороту.

Особенности автоматизированного безбумажного документооборота. Единство принципов и направлений движения традиционных и электронных документов. Стабильная для всех типов носителей информации структура документооборота.

Типовой состав технологических стадий входного (входящего, поступающего), выходного (отправляемого, исходящего) и внутреннего документопотоков.

Анализ угроз несанкционированного получения документированной информации, хищения или уничтожения документов, их фальсификации или подмены в документопотоках. Классификация каналов практической реализации возможных угроз. Предполагаемые рубежи и уровни защиты документопотоков.

Понятие защищенного документооборота, его цели и задачи. Взаимосвязь защищенного документооборота с системами, средствами и методами защиты документированной информации. Защищенный документооборот и используемая технологическая система обработки и хранения документов. Цели и принципы функциональной и персональной избирательности в доставке документированной информации потребителям. Избирательность и разрешительная система доступа к конфиденциальным документам и базам данных. Персональная ответственность за сохранность информации, носителя информации и документа.

Выделенный поток конфиденциальных документов и автономная технология их обработки и хранения. Организационные и технологические особенности делопроизводства по конфиденциальным документам.

Пооперационный учет движения конфиденциальных документов и доступа к ним руководителей и специалистов. Учет чистых носителей информации, предназначенных для документирования конфиденциальной информации. Периодические и разовые проверки наличия конфиденциальных документов.

Потоки конфиденциальных документов. Принципы защиты документопотоков, защищенная технология.

Уровень конфиденциальности информации. Организационное обеспечение защиты потоков документированной информации. Принципы, способы и средства защиты технических носителей информации и машиночитаемых документов на разных стадиях их обработки, движения и хранения.

Стадии обработки и защиты конфиденциальных документов входного потока

Назначение и задачи стадии приема и первичной обработки конфиденциальных документов. Типовой состав операций процедуры приема пакетов, конвертов и иных отправлений, поступивших из почтового отделения или от нарочного. Учет поступлений, состав фиксируемых данных. Типовой состав операций процедуры первичной обработки документов. Назначение и задачи стадии предварительного рассмотрения и распределения поступивших документов. Типовой состав операций процедуры предварительного рассмотрения документов.

Порядок определения рационального маршрута движения документа. Принципы распределения документов между руководителями, структурными подразделениями и специалистами. Функциональная принадлежность документированной информации. Уровень компетенции должностных лиц при решении вопросов, поставленных в документах. Реализация порядка доступа к документам. Типовой состав операций процедуры распределения поступивших документов.

Назначение и задачи стадии учета поступивших документов. Однократность регистрации документа. Состав процедур стадии учета документов.

Типовой состав операций процедуры первичной регистрации исходных сведений о документе. Носители записи исходных сведений о документе.

Журналы учета (регистрации) документов. Регистрационно-контрольные карточки. Правила заполнения граф и зон учетной формы.

Задачи и порядок ведения журналов учета и картотек. Обоснование состава дополнительно регистрируемых сведений, их назначение. Правила внесения изменений и дополнений в имеющиеся записи.

Типовой состав операций процедуры рассмотрения документов руководителем. Требования к формулированию заданий, поручений по исполнению документа и определению состава исполнителей и сроков исполнения. Правила работы руководителя и его референта с конфиденциальными документами, порядок хранения документов на их рабочих местах.

Типовой состав операций процедуры передачи документов на исполнение. Порядок доведения до исполнителя содержания конфиденциального документа и резолюции руководителя. Порядок передачи документа на исполнение нескольким структурным подразделениям или специалистам. Порядок перемещения документа между руководителями и специалистами. Типовой состав учетных операций.

*Стадии обработки и защиты конфиденциальных документов выходного поток*а

Назначение и задачи стадии исполнения документов. Понятие исполнение документа, инициирующие условия начала исполнения. Состав процедур.

Типовой состав операций процедуры составления текста документа. Состав, особенности применения и оформления, учет бумажных и технических носителей информации. Критерии и порядок определения степени конфиденциальности документов, изменения и снятия грифа. Типовой состав операций процедуры изготовления документа. Машинописное оформление конфиденциального документа. Типовой состав учетных операций при печатании и перепечатывании проекта документа, передаче печатного материала исполнителю. Формы учета и правила их заполнения. Порядок уничтожения черновика документа, испорченных листов и сопутствующих материалов. Оформление результатов уничтожения. Правила печатания под диктовку и с диктофона.

Типовой состав операций процедуры издания документа. Технология согласования, подписания, утверждения документа.

Документирование санкционирования доступа персонала к базам данных, учет доступа. Опись документов и носителей информации, находящихся у спе-

циалиста. Правила работы специалиста с конфиденциальными документами, порядок обеспечения сохранности документов на его рабочем месте.

Назначение и задачи стадии контроля исполнения документов. Контроль сроков исполнения документов, заданий и поручений. Контроль предупредительный (текущий) и последующий (итоговый). Задачи и сферы защиты информации в процессе контроля исполнения документов. Состав контролируемых документов и сроки их исполнения. Типовой состав операций процедуры постановки документов на контроль. Типовой состав операций процедуры ведения контроля. Напоминания исполнителям и справочная работа по контролируемым документам.

Назначение и задачи стадии копирования и размножения документов. Учет документов. Типовой состав операций процедуры оформления результатов копирования или размножения.

Учет изготовленных экземпляров документа. Порядок уничтожения печатных форм, брака и документирование результатов уничтожения в соответствии с уровнем грифа конфиденциальности. Назначение и задачи стадии учета отправляемых и внутренних документов. Централизация учета. Состав процедур. Состав фиксируемых сведений об отправляемых инициативном и ответном документах, о внутреннем документе. Обоснование состава сведений, назначение и сфера последующего использования каждого показателя.

Процедура передачи внутренних документов для исполнения или использования.

Типовой состав операций процедуры подготовки и передачи отправляемых документов для экспедиционной обработки. Назначение и задачи стадии экспедиционной обработки отправляемых документов. Типовой состав операций процедуры контроля комплектности документов. Типовой состав операций процедуры конвертования документов. Правила оформления конвертов (пакетов) с конфиденциальными документами. Типовой состав операций процедуры передачи конвертов (пакетов) нарочным или в почтовое отделение. Оформление реестров. Прядок документирования факта передачи нарочным конверта (пакета) адресату. Правила отправления телеграмм, телефаксов и телетайпограмм.

Систематизация и оперативное хранение конфиденциальных документов и дел

Назначение и задачи стадии составления и ведения номенклатуры дел. Методика составления номенклатуры дел: изучение состава документов, разработка классификационной схемы номенклатуры, формулирование заголовков дел и их систематизация, индексирование дел, определение сроков хранения дел. Правила формулирования заголовков дел. Перечень документов с указанием сроков их хранения. Назначение перечня. Типовые и ведомственные перечни. Оформление номенклатуры дел, ее согласование и утверждение. Типовой состав операций процедуры ведения и закрытия номенклатуры дел.

Назначение и задачи стадии формирования и оперативного хранения дел. Понятие формирование дел. Единство регистрационного индекса и места хранения документа. Типовой состав операций процедуры формирования дел. Заведение дел постоянного и временного сроков хранения, оформление обложки дела. Требования, предъявляемые к группировке документов в дела. Технологические

операции группировки. Разложение документов внутри дела. Особенности формирования личных дел. Дополнительные требования к формированию в дела конфиденциальных документов. Нумерация листов. Заполнение описи документов дела. Составление заверительной надписи. Прошивка и опечатывание дела. Оформление карточки учета выдачи дела. Типовой состав операций процедуры хранения дел. Правила хранения документов, выдачи и приема дел, изъятие документов из дела.

Назначение и состав документов и дел выделенного хранения. Формы учета и содержания регистрируемых сведений. Технологические операции перевода документов и дел на выделенное хранение.

Назначение и задачи стадии подготовки и передачи дел в архив. Процедура экспертизы ценности документов. Понятие «экспертиза ценности документов», ее задачи, принципы и критерии. Требования, предъявляемые к экспертизе. Организация проведения экспертизы ценности документов. Задачи, функции, состав и порядок работы экспертной комиссии. Этапы проведения экспертизы ценности документов. Типовой состав операций каждого этапа. Дополнительные требования к проведению экспертизы ценности конфиденциальных документов. Оформление результатов экспертизы.

Назначение и виды описей дел. Порядок составления описи, ее оформление, согласование и утверждение. Типовой состав операций процедуры подготовки дел к передаче в архив. Типовой состав операций процедуры передачи дел в архив.

Назначение и задачи стадии уничтожения документов и носителей информации. Процедура отбора документов и носителей информации для уничтожения. Организация и порядок отбора. Типовой состав операций. Оформление результатов отбора. Порядок составления и оформления акта о выделении к уничтожению документов, не подлежащих хранению. Требования по включению в акт документов, дел и носителей информации. Подготовка к уничтожению бумажных, машиночитаемых, аудиовизуальных, конструкторских, технологических и научно-технических документов. Процедура уничтожения документов и носителей информации. Требования к процессу уничтожения документов в соответствии со степенью их конфиденциальности. Порядок внесения отметок об уничтожении документов и носителей информации в учетные формы. Средства организационной техники, используемые при выполнении процедуры.

Проверка наличия конфиденциальных документов, дел и носителей информации

Назначение и задачи проверки наличия документов, дел и носителей информации. Сферы распространения проверки. Требования, предъявляемые к проверке. Виды проверок. Периодичность проверок наличия и уровень конфиденциальности информации. Проверки регламентированные (периодические) и нерегламентированные (непериодические). Типовой состав процедур и операций проверки наличия.

Организация поиска отсутствующих конфиденциальных документов. Специализированная комиссия для установления причин отсутствия документов.

Оформление заключения о результатах работы комиссии. Списание документов, отметки в учетных формах.

Текущая проверка наличия документов, дел и носителей информации. Ее цели, состав проверяемых документов. Оформление результата проверки.

Квартальная и годовая проверки наличия документов, дел и носителей информации. Цели проверок и состав проверяемых документов. Оформление результатов проверок.

Ежемесячная проверка наличия особо важных конфиденциальных документов. Ее цели, состав проверяемых документов. Оформление результата проверки.

Проверка наличия документов, дел и носителей информации при увольнении сотрудника. Ее цели и оформление результата проверки. Порядок приема от увольняющегося документов, дел и носителей информации. Оформление результата приема.

Проверки наличия и сохранности баз данных в ЭВМ. Цели проверки и порядок ее проведения. Оформление результата проверки.

Предпосылки нерегламентированных проверок наличия документов, дел и носителей информации. Цели проверки, состав проверяемых документов и оформление результата проверки.

Политика информационной безопасности предприятия

Основные цели и задачи системы организационной защиты информации. Угрозы информационной безопасности. Внутренние и внешние угрозы. Случайные и преднамеренные угрозы. Организационные меры противодействия угрозам. Каналы утечки информации

Концепция информационной безопасности предприятия. Структура и требования по информационной безопасности предприятия. Процедуры и методы информационной безопасности предприятия. Особенности информационной защиты компьютерных сетей. Реализация принципа разделения полномочий.

Работа с персоналом, допущенным к конфиденциальной информации

Задачи и направления работы с персоналом. Особенности приема сотрудников на работу. Критерии подбора персонала, процедуры подбора и документирования приема. Учет психологических особенностей сотрудников, принимаемых на работу. Обязательство о неразглашении тайны. Особенности увольнения сотрудников с работы. Процедуры увольнения и их документирование. Направления и методы текущей работы с персоналом. Инструктирование и обучение сотрудников, задачи, принципы и способы. Меры поощрения и наказания, используемые для поддержания дисциплины сотрудников, допущенных к работе с конфиденциальной информации.

Организационная защита информации в процессе проведения совещаний и переговоров по конфиденциальным вопросам

Задачи и направления защиты информации в процессе проведения совещаний и переговоров, а также при приеме посетителей. Требования к отбору информации для ее оглашения в процессе переговоров. Правила подготовки и проведения совещаний и переговоров. Документирование информации, оформление стенограмм, протоколов и итоговых документов. Порядок использования аудио- и ви-

деозаписи хода переговоров. Требования к помещениям и их охране. Обязанности лиц, ответственных за проведение совещаний и переговоров. Методы контроля за действиями посетителей. Требования к помещениям для приема посетителей.

Организация защиты информации в автоматизированных информационных системах, обрабатывающих конфиденциальную информацию

Стадии создания информационных систем. Порядок организационной защиты информации в процессе проектирования, пуско-наладочных работ и эксплуатации информационных систем. Организация защиты информации при выходе в сети общего пользования. Порядок аттестации объектов информатизации и информационных систем, обрабатывающих конфиденциальную информацию.

Организационная защита информации при взаимодействии со сторонними организациями в процессе договорной, выставочной, рекламной и иной внешней деятельности предприятия

Угроза информационной безопасности при взаимодействии со сторонними организациями. Порядок отбора и подготовки информации к оглашению. Отражение вопросов защиты информации при подготовке договоров. Виды публикации информации. Оформление разрешения на опубликование информации. Особенности обеспечения безопасности информации в процессе выставочной деятельности.

Порядок установления пропускного и объектового режимов

Виды, назначение и задачи охраны объектов. Состав функции охраны. Построение системы охраны объекта, рубежи охраны. Регламентация деятельности, обязанностей и ответственности персонала охраны. Взаимодействие персонала с техническими средствами сигнализации, информирования и идентификации. Порядок сдачи под охрану и снятия с охраны объектов и режимных помещений. Назначение и задачи пропускного режима. Понятие, задачи и структура пропускного и объектового режима. Порядок организации доступа персонала в помещения различной категории. Функционирование контрольно-пропускных пунктов. Виды пропусков и идентификаторов, их учет и порядок выдачи.

Порядок допуска и доступа персонала и иных лиц к конфиденциальной информации

Назначение, принципы и задачи разрешительной системы допуска и доступа к информации ограниченного доступа. Структура разрешительной системы. Назначение и формы допусков, порядок оформления, учета и хранения. Несанкционированный доступ. Порядок оформления разрешения на доступ, мандатная и матричная системы доступа. Порядок доступа к информации ограниченного доступа лиц, командированных другими организациями. Особенности доступа к конфиденциальной информации.

Аналитическая и плановая работа в сфере организационной защиты информации

Контроль состояния информационной безопасности. Назначение и взаимосвязь аналитической, плановой и контрольной работы, ее место в построении и функционировании системы организационной защиты информации. Цели и задачи аналитической работы по выявлению угроз безопасности информации. Этапы

аналитической работы. Оценка надежности информационной защиты. Цели и задачи планирования мероприятий по формированию и совершенствованию системы организационной защиты информации. Виды программ и планов. Контроль за выполнением программ и планов. Аудит информационной безопасности. Методы прогнозирования и верификации состояния безопасности информации.

Организация служебного расследования по фактам утраты конфиденциальной информации

Цели и задачи служебного расследования. Основания для служебного расследования. Меры, принимаемые по результатам расследования. Документирование хода и результатов служебного расследования. Порядок проведения служебного расследования в случаях возникновения сложных инцидентов. Особенности проведения служебного расследования инцидентов, происшедших в компьютерных сетях.

Организационные меры по обеспечению и поддержанию информационной безопасности в период чрезвычайных ситуаций

Виды и характерные особенности чрезвычайных ситуаций. Этапы развития чрезвычайных ситуаций. Основные задачи по поддержанию информационной безопасности в период чрезвычайных ситуаций. Кризисные группы. Планирование и проверка готовности подразделений предприятий к действиям период чрезвычайных ситуаций. Особенности подготовки распорядительных документов по действиям сотрудников, обеспечивающих безопасность информации на период чрезвычайных ситуаций. Организационные меры, принимаемые на предприятии по обеспечению пожарной безопасности. Порядок восстановления целостности и доступности информации в период после окончания чрезвычайной ситуации.