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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ И ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

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

Информационная безопасность распределенных информационных систем и центров обработки данных: 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.

© КузГТУ, 2018

© Е. В. Прокопенко,
И. В. Чичерин,
составление, 2018

1.Исходные понятия и определения

Под распределенными понимаются КС, которые не располагаются на одной контролируемой территории, на одном объекте.

В общем случае, ***распределенная компьютерная система*** (РКС) представляет собой множество сосредоточенных КС, связанных в единую систему с помощью коммуникационной подсистемы.

Сосредоточенными КС могут быть отдельные ЭВМ, в т. ч. и ПЭВМ, вычислительные системы и комплексы, а также локальные вычислительные сети (ЛВС).

Архитектура распределенных кс.

Наименьшей структурной единицей РКС является ЭВМ.

Распределенные КС строятся по сетевым технологиям и представляют собой вычислительные сети (ВСт). Коммутационная подсистема включает:

- ***коммутационные модули*** (КМ) (их основная функция – передача полученного пакета другому КМ или абонентскому пункту в соответствии с маршрутом передачи. Коммутационный модуль называют также центром коммутации пакетов);

- ***каналы связи*** (объединяют элементы сети в единую сеть. Каналы могут иметь различную скорость передачи данных);

- ***концентраторы*** (используются для уплотнения информации перед передачей ее по высокоскоростным каналам);

- ***межсетевые шлюзы*** (мосты) (используются для связи сети с ЛВС или для связи сегментов глобальных сетей. С помощью мостов связываются сегменты сети с одинаковыми сетевыми протоколами).

В любой РКС в соответствии с функциональным назначением может быть выделено три подсистемы:

- пользовательская (абонентская) подсистема (включает в себя компьютерные системы пользователей (абонентов) и предназначается для удовлетворения потребностей пользователей в хранении, обработке и получении информации);

- подсистема управления (позволяет объединить все элементы РКС в единую систему, в которой взаимодействие элементов осуществляется по единым правилам. Подсистема обеспечивает взаимодействие элементов системы путем сбора и анализа служебной информации и воздействия на элементы с целью создания оптимальных условий для функционирования всей сети);

- коммуникационная подсистема (обеспечивает передачу информации в сети в интересах пользователей и управления РКС).

2. Распределенные компьютерные сети

В течение последних шестидесяти лет информационные технологии претерпели кардинальные изменения. Начиная от больших ламповых вычислительных машин и заканчивая современными персональными компьютерами и промышленными серверами. Техническая мысль стремительно развивалась, рождая тем самым новое. Одной из таких новинок было изобретение высокоскоростных

компьютерных сетей. Они позволили строить различные системы связанных между собой устройств передачи и обработки информации.

Определение. Распределенная система – это набор независимых компьютеров, представляющийся их пользователям единой объединенной системой.

Распределенные системы должны иметь возможность поддаваться расширению, или масштабированию. Эта характеристика является прямым следствием наличия независимых компьютеров, но в то же время не указывает, каким образом эти компьютеры на самом деле объединяются в единую систему. Распределенные системы обычно существуют постоянно, однако некоторые их части могут временно выходить из строя. Пользователи и приложения не должны уведомляться о том, что эти части заменены или починены или что добавлены новые части для поддержки дополнительных пользователей или приложений.

Распределенная система должна обладать несколькими важными свойствами, в числе которых прозрачность, открытость, масштабируемость.

Важная задача, выполнение которой обеспечивает прозрачность, состоит в том чтобы нивелировать факт распределения программных и аппаратных ресурсов по множеству компьютеров. Распределенная система представляется пользователям как единая совокупность, т.е. она является прозрачной (transparent).

Концепция прозрачности затрагивает различные вопросы функционирования распределенных систем. Основные аспекты функционирования распределенной вычислительной системы:

- ✓ **Доступ** – Скрывается разница в представлении данных и доступе к ресурсам.
- ✓ **Местоположение** – Скрывается местоположение ресурса.
- ✓ **Перенос** – Скрывается факт перемещения ресурса в другое место.
- ✓ **Смена местоположения** – Скрывается факт перемещения ресурса в процессе обработки в другое место.
- ✓ **Репликация** – Скрывает факт репликации ресурса.
- ✓ **Параллельный доступ** – Скрывается факт возможного совместного использования.
- ✓ **Отказ** – Скрывает отказ и восстановление ресурса.
- ✓ **Сохранность** – Скрывается, хранится ресурс (программный) на диске или находится в оперативной памяти.

Также важной характеристикой распределенных систем является открытость.

Определение. Открытая распределенная система — это система, предлагающие службы, вызов которых требует стандартный синтаксис и семантику. Примером может служить компьютерная сеть, взаимодействие между узлами которой происходит посредством единых протоколов.

С расширением компьютерных систем большое значение приобретает такая характеристика, как масштабируемость.

Масштаб системы может измеряться по различным показателям:

1) система может масштабироваться по отношению к её размеру;

2) система может масштабироваться географически, пользователи и набор сервисов могут быть разнесены в пространстве;

3) система может быть разнесена в административном смысле, то есть работать в различных административно разделенных организациях.

Но вместе с тем возникают достаточно серьезные проблемы, связанные с обеспечением информационной безопасности.

Рассмотрим архитектуру распределенной компьютерной системы более подробно. В первом приближении РКС – это системы находится на различных территориально разрозненных узлах. Структура системы строится по принципам сетевых технологий.

Подсистема передачи информации в распределенной компьютерной системе включает в себя следующие компоненты:

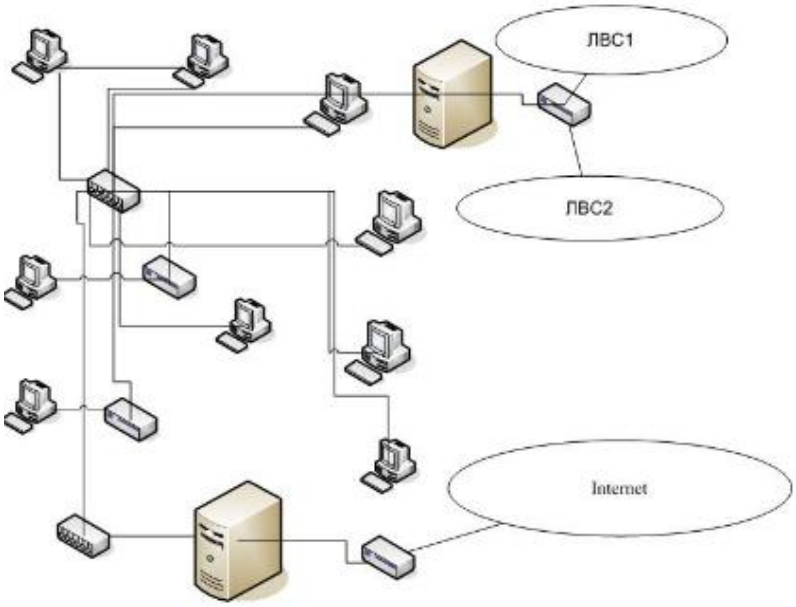
- ✓ коммутационные модули;
- ✓ каналы связи;
- ✓ концентраторы;
- ✓ межсетевые шлюзы.

Коммутационные модули предназначены для передачи входящих пакетов к другому КМ в соответствии с маршрутом передачи. Каналы связи соединяют узлы в сети. У каналов могут быть различные скорости передачи данных. Концентраторы используются для компоновки информации с целью ее передачи по каналам связи. Межсетевые шлюзы и мосты используются для связи в компьютерной сети или ее территориально разрозненных сегментов.

В соответствии с назначением РКС может быть выделено три подсистемы:

- ✓ пользовательская подсистема;
- ✓ подсистема управления;
- ✓ коммуникационная подсистема.

Пользовательская подсистема содержит в себе компьютерные системы пользователей и предназначается для обработки, хранения и передачи информации.



Сегмент распределенной компьютерной системы

Подсистема управления играет роль связующего звена РКС в единую систему, в которой взаимодействие элементов производится по единым правилам. Она обеспечивает взаимодействие элементов системы путем сбора и анализа служебной информации и воздействие на элементы с целью создания оптимальных условий для функционирования всей сети в целом.

Коммуникационная подсистема делает возможной передачу информации в сети, позволяя управлять РКС.

Рассмотрим основные особенности информационной безопасности в распределенной компьютерной системе. РКС подразделяются на корпоративные и общедоступные. В *корпоративных системах* все составные части принадлежат одной организации. В таких системах имеется возможность проводить единую политику обеспечения безопасности. В общедоступных системах единое обеспечение безопасности затрудненно введу неоднородности. Таким образом, меры по обеспечению стабильности работы и защиты информационных ресурсов решается на уровне конечных пользователей.

Специалисты, выполняя проектирование системы защиты информации для РКС, должны учитывать следующее:

- ✓ сложность системы, которая определяется как количеством подсистем, так и разнообразием их типов и выполняемых функций;
- ✓ невозможность обеспечения эффективного контроля за доступом к ресурсам, распределенным на больших расстояниях, возможно за пределами границ страны;
- ✓ возможность принадлежности ресурсов сети различным владельцам.

Особенностью защиты информации от непреднамеренных угроз в РКС по сравнению с сосредоточенными сетями является необходимость обеспечения гарантированной передачи информации по коммуникационной подсети. Для этого в РКС должны быть предусмотрены дублирующие маршруты доставки сообщений, предприняты меры против искажения и потери информации в каналах связи. Такие сложные системы должны строиться как адаптивные, в которых обеспечивается постоянный контроль работоспособности элементов системы и возможность продолжения функционирования даже в условиях отказов отдельных подсистем.

В распределенных компьютерных системах угрозы информационной безопасности делятся на пассивные и активные.

Пассивные угрозы – это угрозы целью, которых является получение информации о системе во время прослушивания каналов передачи информации. Активные угрозы предусматривают воздействие на передаваемые сообщения и несанкционированную передачу информации по сети. Такая передача информации может частично или полностью вывести из строя РКС.

Можно сделать вывод о том, что все особенности угроз безопасности в РКС связаны непосредственно передачей информации и с разрозненностью в пространстве частей системы. Таким образом, в распределенной компьютерной системе реализуются механизмы информационной безопасности при передаче по каналам связи и механизмы защиты от несанкционированного воздействия на информацию в системе.

Для защиты данных, передаваемых по каналам связи, применяется комплекс методов, позволяющих блокировать возможные угрозы. Наиболее надежным и универсальным методом защиты информации в каналах связи является шифрование. Шифрование на абонентском уровне позволяет защитить рабочую информацию от утраты конфиденциальности и навязывания ложной информации. Линейное шифрование позволяет, кроме того, защитить служебную информацию. Не имея доступа к служебной информации, злоумышленник не может фиксировать факт передачи между конкретными абонентами сети, изменить адресную часть сообщения с целью его переадресации.

Различают различные способы защиты информации при передаче ее по каналам связи.

Установка межсетевых экранов позволяет с помощью общедоступно распределенной компьютерной системы связать воедино различные скрытые сегменты корпоративной системы предприятия.

Обеспечение подтверждения подлинности взаимодействующих процессов позволяет определить те процессы, с которыми процессы РКС или другой системы могут безопасно взаимодействовать.

При обеспечении безопасности в распределенных компьютерных системах необходимо обеспечить реализацию различных защитных механизмов. Однако если раньше большая часть усилий была сконцентрирована на развитии криптографических методов, то текущее состояние развития информационно-безопасных РКС, а также на другие механизмы защиты, и, в первую очередь, на разработку методов активного аудита безопасности компьютерных систем[i].

3. Защита информации в распределенных компьютерных сетях

С точки зрения защиты информации в РКС важно разделить вычислительные сети на корпоративные и общедоступные.

В корпоративных сетях все элементы принадлежат одному ведомству, за исключением, может быть, каналов связи. В таких системах имеется возможность проводить единую политику обеспечения безопасности информации по всей сети.

В общедоступных коммерческих сетях во главу угла ставится распространение информации, а вопросы защиты собственных информационных ресурсов решаются, в основном, на уровне пользователей.

Корпоративные сети могут быть связаны с общедоступными сетями. В этом случае администрации (владельцам) корпоративных сетей необходимо предпринимать дополнительные меры предосторожности для блокирования возможных угроз со стороны общедоступных сетей.

При построении системы защиты информации в любой РКС необходимо учитывать:

- сложность системы, которая определяется как количеством подсистем, так и разнообразием их типов и выполняемых функций;

- невозможность обеспечения эффективного контроля за доступом к ресурсам, распределенным на больших расстояниях, возможно за пределами границ страны;

- возможность принадлежности ресурсов сети различным владельцам.

Особенностью защиты информации от непреднамеренных угроз в РКС по сравнению с сосредоточенными сетями является необходимость обеспечения гарантированной передачи информации по коммуникационной подсети. Для этого в РКС должны быть предусмотрены дублирующие маршруты доставки сообщений, предприняты меры против искажения и потери информации в каналах связи. Такие сложные системы должны строиться как адаптивные, в которых обеспечивается постоянный контроль работоспособности элементов системы и возможность продолжения функционирования даже в условиях отказов отдельных подсистем.

Искажения информации в каналах связи фиксируются и частично исправляются с помощью помехоустойчивого кодирования. Потери информации исключаются за счет использования контроля и учета принятых сообщений, а также за счет применения протоколов обмена с подтверждением о приеме информации.

В РКС все потенциальные преднамеренные угрозы безопасности информации делят на две группы: пассивные и активные.

К ***пассивным*** относятся угрозы, целью реализации которых является получение информации о системе путем прослушивания каналов связи (злоумышленник может получить информацию путем перехвата незашифрованных сообщений или путем анализа трафика (потока сообщений), накапливая информацию об интенсивности обмена отдельных абонентов, о структуре сообщений, о маршрутах доставки сообщений и т. п.).

Активные угрозы предусматривают воздействие на передаваемые сообщения в сети и несанкционированную передачу фальсифицированных сообщений с целью воздействия на информационные ресурсы объектов РКС и дестабилизацию функционирования системы. Возможно также непосредственное воздействие на коммуникационную подсистему с целью повреждения аппаратных средств передачи информации.

Передаваемые в РКС сообщения могут несанкционированно модифицироваться или уничтожаться. Злоумышленник может размножать перехваченные сообщения, нарушать их очередность следования, изменять маршрут доставки, подменять сообщения, может предпринимать попытки несанкционированного доступа к информационным ресурсам удаленного объекта КС, осуществления несанкционированного изменения программной структуры КС путем внедрения вредительских программ.

В РКС все угрозы связаны с передачей информации по каналам связи, с территориальной разобщенностью объектов системы.

Поэтому, в РКС, наряду с мерами, предпринимаемыми для обеспечения безопасности информации в сосредоточенных КС, реализуется ряд механизмов для защиты информации при передаче ее по каналам связи, а также для защиты от несанкционированного воздействия на информацию КС с использованием КС.

Все методы и средства, обеспечивающие безопасность информации в защищенной вычислительной сети, могут быть распределены по группам:

- обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных КС;

- защита информации на уровне подсистемы управления сетью;
- защита информации в каналах связи;
- обеспечение контроля подлинности взаимодействующих процессов.

4. Пользовательские подсистемы

Особенностью защиты объектов РКС является необходимость поддержки механизмов аутентификации и разграничения доступа удаленных процессов к ресурсам объекта, а также наличие в сети специальных коммуникационных компьютерных систем.

Все элементы коммуникационной подсистемы, за исключением каналов связи, рассматриваются как специализированные коммуникационные компьютерные системы. В защищенных корпоративных сетях концентраторы, коммуникационные модули (серверы), шлюзы и мосты целесообразно размещать на объектах совместно с КС пользователей. Особенностью всех коммуникационных КС является информация, которая обрабатывается этими системами. В таких системах имеется принципиальная возможность не раскрывать содержание рабочей информации. Она не должна быть доступной операторам и другому обслуживающему персоналу коммуникационных компьютерных систем для просмотра на экране монитора, изменения, уничтожения, размножения, запоминания в доступной памяти, получения твердой копии. Такая информация не должна сохраняться на внешних запоминающих устройствах после успешной передачи сообщения другому элементу коммуникационной подсистемы. В закрытых системах рабочая информация, кроме того, в пределах коммуникационной подсети циркулирует в зашифрованном виде.

Различают два вида шифрования в КС:

- ***линейное*** – шифрование в коммуникационной подсистеме (на входе в коммуникационную подсистему сообщение подвергается линейному зашифрованию, даже если абонентское зашифрование и не выполнялось – сообщение зашифровывается полностью, включая все служебные данные. Причем, линейное зашифрование может осуществляться в сети с разными ключами, а значит рабочая информация остается зашифрованной на абонентском уровне);
- ***абонентское*** – межконцевое шифрование (абонент перед отправкой осуществляет зашифрование сообщения с помощью симметричного или открытого ключа).

Особое внимание должно уделяться центру управления сетью. Учитывая концентрацию информации, критичной для работы всей сети, необходимо использовать самые совершенные средства защиты информации специализированной КС администратора сети как от непреднамеренных, так и от преднамеренных угроз. Особое внимание – защите процедур со средств, связанных с хранением и работой с ключами.

Администратор сети как и все операторы коммуникационной подсети, работает только со служебной информацией. Однако в специализированной КС администратора сети должны быть предусмотрены механизмы, блокирующие воз-

можность работы с информационной частью сообщений, которые не предназначаются администратору.

5. Подсистема управления

Управление передачей сообщений осуществляется по определенным правилам, которые называются протоколами. В настоящее время в распределенных вычислительных сетях реализуются два международных стандарта взаимодействия удаленных элементов сети: протокол **TCP/IP** и протокол **X.25**.

На основе протокола **TCP/IP** построена сеть Internet. Протокол **X.25** явился дальнейшим развитием технологии передачи данных, построенной на основе коммутации пакетов. Протокол **X.25** соответствует модели стандартизации OSI/ISO, в соответствии с моделью которой все функции разбиваются на 7 уровней (в модели TCP/IP насчитывается 5 уровней).

Модель OSI: Модель TCP/IP:

- прикладной;
- представительский; – прикладной;
- сеансовый;
- транспортный; – транспортный;
- сетевой; – сетевой;
- канальный; – канальный;
- физический. – физический.

Протокол **X.25** позволяет обеспечить более надежное взаимодействие удаленных процессов.

Достоинствами протокола **TCP/IP** является сравнительно низкая стоимость и простота подключения к сети.

Задачи обеспечения безопасности информации в сети решаются на всех уровнях. Выполнение протоколов организуется с помощью подсистемы управления. Наряду с другими на уровне подсистемы управления решаются следующие проблемы защиты информации в РКС:

- создание единого центра управления сетью, в котором решались бы и вопросы обеспечения безопасности информации. Администратор и его аппарат проводят единую политику безопасности во всей защищенной сети;
- регистрация всех объектов сети и обеспечение их защиты. Выдача идентификаторов и учет всех пользователей сети;
- управление доступом к ресурсам сети;
- генерация и рассылка ключей шифрования абонентам компьютерной сети;
- мониторинг трафика (потока сообщений в сети), контроль соблюдения правил работы абонентами, оперативное реагирование на нарушения;
- организация восстановления работоспособности элементов сети при нарушении процесса их функционирования.

6. Каналы связи

Для защиты информации, передаваемой АО каналам связи, применяется комплекс методов и средств защиты, позволяющих блокировать возможные угрозы безопасности информации.

Наиболее надежным и универсальным методом защиты информации в каналах связи является шифрование.

Шифрование на абонентском уровне позволяет защитить рабочую информацию от утраты конфиденциальности и навязывания ложной информации.

Линейное шифрование позволяет, кроме того, защитить служебную информацию. Не имея доступа к служебной информации, злоумышленник не может фиксировать факт передачи между конкретными абонентами сети, изменить адресную часть сообщения с целью его переадресации.

Противодействие ложным соединениям абонентов (процессов) обеспечивается применением целого ряда процедур взаимного подтверждения подлинности абонентов или процессов. Против удаления, явного искажения, переупорядочивания, передачи дублей сообщений используется механизм квитирования, нумерации сообщений или использования информации о времени отправки сообщения. Эти служебные данные должны быть зашифрованы.

Интенсивность обмена может быть скрыта путем добавления к рабочему трафику обмена специальными сообщениями.

Попыткам блокировки коммуникационной подсистемы путем интенсивной передачи злоумышленником сообщений или распространения вредительских программ типа с «червь», в подсистеме управления РКС должны быть созданы распределенные механизмы контроля интенсивности обмена и блокирования доступа в сеть абонентов при исчерпании ими лимита активности или в случае угрожающего возрастания трафика. Для блокирования угроз физического воздействия на каналы связи (нарушение линий связи или постановка помех в радиоканалах) необходимо иметь дублирующие каналы с возможностью автоматического перехода на их использование.

7. Базы данных

Базы данных рассматриваются как надежное хранилище структурированных данных, снабженное специальным механизмом для их эффективного использования в интересах пользователей (процессов). Таким механизмом является СУБД – система управления базой данных, под которой понимаются программные или аппаратно-программные средства, реализующие функции управления данными, такие как: просмотр, сортировка, выборка, модификация, выполнение операций определения статистических характеристик и т. п.

Базы данных размещаются на:

- компьютерной системе пользователя;
- специально выделенной ЭВМ (сервере).

В вычислительных сетях базы данных размещаются на серверах. В локальных и корпоративных сетях, как правило, используются централизованные базы

данных. Общедоступные глобальные сети имеют распределенные базы данных, а серверы в таких сетях размещаются на различных объектах системы.

В централизованных базах данных проще решаются проблемы защиты информации от преднамеренных угроз, поддержания актуальности и непротиворечивости данных. Достоинством распределенных баз данных, при условии дублирования данных, является их высокая защищенность от стихийных бедствий, аварий, сбоев технических средств, а также диверсий.

Защита информации в базах данных, в отличие от защиты данных в файлах, имеет и свои особенности:

- необходимость учета функционирования системы управления базой данных при выборе механизмов защиты;
- разграничение доступа к информации реализуется не на уровне файлов, а на уровне частей баз данных.

При создании средств защиты информации в базах данных необходимо учитывать взаимодействие этих средств не только с ОЧС, но и с ЧСУБД. При этом возможно встраивание механизмов защиты в СУБД или использование их в виде отдельных компонент.

В современных базах данных довольно успешно решаются задачи разграничения доступа, поддержания физической целостности и логической сохранности данных. Разграничение доступа к файлам баз данных и к частям баз данных осуществляется СУБД путем установления полномочий пользователей и контроля этих полномочий при допуске к объектам доступа.

Полномочия пользователей устанавливаются администратором СУБД. Обычно стандартным идентификатором пользователя является пароль, передаваемый в зашифрованном виде. В распределенных КС процесс подтверждения подлинности пользователя дополняется специальной процедурой взаимной аутентификации удаленных процессов. Базы данных, содержащих конфиденциальную информацию, хранятся на внешних запоминающих устройствах в зашифрованном виде.

Физическая целостность баз данных достигается путем использования отказоустойчивых устройств, построенных, например, по технологии RAID. Логическая сохранность данных означает невозможность нарушения структуры модели данных. Современные СУБД обеспечивают такую логическую целостность и непротиворечивость на этапе описания модели данных.

В базах данных, работающих с конфиденциальной информацией необходимо дополнительно использовать криптографические средства закрытия информации. Для этой цели используется шифрование как с помощью единого ключа, так и с помощью индивидуальных ключей пользователей.

Возможны два режима работы с зашифрованными базами данных.

Первый – при выполнении запроса необходимый файл или часть файла расшифровывается на внешнем носителе, с открытой информацией производятся необходимые действия, после чего информация на ВЗУ снова зашифровывается. Достоинства – независимость функционирования средств шифрования в СУБД, которые работают последовательно друг за другом. В то же время сбой или отказ

в системе может привести к тому, что на ВЗУ часть базы данных останется записанной в открытом виде.

Второй – возможность выполнения СУБД запросов пользователей без расшифровывания информации на ВЗУ. Поиск необходимых файлов, записей, полей, групп полей не требует расшифрования. Расшифрование производится в ОП непосредственно перед выполнением конкретных действий с данными. Такой режим возможен, если процедуры шифрования встроены в СУБД. При этом достигается высокий уровень защиты от несанкционированного доступа, но реализация режима связана с усложнением СУБД.

Противодействие угрозам информации в базах данных осуществляется следующими методами:

- блокировкой ответа при неправильном числе запросов;
- искажением ответа путем округления и другой преднамеренной коррекции данных;
- разделением баз данных;
- случайным выбором записи для обработки;
- контекстно-ориентированной защитой;
- контролем поступающих запросов[ii].

8. Элементы распределенных компьютерных сетей

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

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 безопасности 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.

---

[i] Артюхов Ю. В. Некоторые аспекты информационной безопасности в распределенной компьютерной системе // Молодой ученый. — 2011. — №2. Т.1. — С. 60-62. — URL https://moluch.ru/archive/25/2709/ (дата обращения: 03.11.2018).

[ii] https://studfiles.net/preview/6302621/page:14/