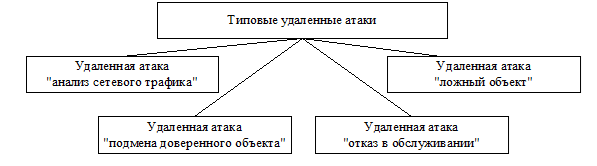
**План-конспект**

**Типовые удаленные атаки в Интернет и механизмы их реализации. Типовые уязвимости, позволяющие реализовать удаленные атаки**

**Типовые удаленные атаки и их характеристика**

Типовая удаленная атака — это удаленное информационное разрушающее воздействие, программно осуществляемое по каналам связи и характерное для любой распределенной вычислительной сети.

**Второстепенные термины**

* ****Удаленная атака «анализ сетевого трафика»
* Удаленная атака «подмена доверенного объекта»
* Удаленная атака «ложный объект»
* Удаленная атака «отказ в обслуживании»

**Расширяющий блок:**Характеристика типовых удаленных атак.

**Структурная схема терминов**

Как уже было показано ранее, распределенные вычислительные сети проектируются на основе одних и тех же принципов, а, следовательно, имеют практически одинаковые проблемы безопасности, причем, в большинстве случаев, независимо от используемых сетевых протоколов, топологии и инфраструктуры вычислительной сети.

С учетом этого специалисты в области информационной безопасности используют понятие типовой удаленной угрозы (атаки), характерной для любых распределенных вычислительных сетей. Введение этого понятия в совокупности с описанием механизмов реализации типовых удаленных угроз позволяет выработать методику исследования безопасности вычислительных сетей, заключающейся в последовательной умышленной реализации всех типовых удаленных угроз и наблюдению за поведением системы.

**Типовая удаленная атак**а — это удаленное информационное разрушающее воздействие, программно осуществляемое по каналам связи и характерное для любой распределенной вычислительной сети.

**3.6.1 Удаленная атака «анализ сетевого трафика»**

Основной особенностью распределенной вычислительной сети является распредельнность ее объектов в пространстве и связь между ними по физическим линиям связи. При этом все управляющие сообщения и данные, пересылаемые между объектами вычислительной сети, передаются по сетевым соединениям в виде пакетов обмена. Эта особенность привела к появлению специфичного для распределенных вычислительных сетей типового удаленного воздействия, заключающегося в прослушивании канала связи, называемого **анализом сетевого трафика**.

Анализ сетевого трафика позволяет:

* изучить логику работы распределенной вычислительной сети, это достигается путем перехвата и анализа пакетов обмена на канальном уровне (знание логики работы сети позволяет на практике моделировать и осуществлять другие типовые удаленные атаки);
* перехватить поток данных, которыми обмениваются объекты сети, т.е. удаленная атака данного типа заключается в получении несанкционированного доступа к информации, которой обмениваются пользователи (примером перехваченной при помощи данной типовой удаленной атаки информации могут служить имя и пароль пользователя, пересылаемые в незашифрованном виде по сети).

По характеру воздействия анализ сетевого трафика является пассивным воздействием (класс 1.1). Осуществление данной атаки без обратной связи (класс 4.2) ведет к нарушению конфиденциальности информации (класс 2.1) внутри одного сегмента сети (класс 5.1) на канальном уровне OSI (класс 6.2). При этом начало осуществления атаки безусловно по отношению к цели атаки (класс 3.3).

3.6.2 Удаленная атака «подмена доверенного объекта»

Одной из проблем безопасности распределенной ВС является недостаточная идентификация и аутентификация  (определение подлинности) удаленных друг от друга объектов. Основная трудность заключается в осуществлении однозначной идентификации сообщений, передаваемых между субъектами и объектами взаимодействия. Обычно в вычислительных сетях эта проблема решается использованием виртуального канала, по которому объекты обмениваются определенной информацией, уникально идентифицирующей данный канал. Для адресации сообщений в распределенных вычислительных сетях используется сетевой адрес, который уникален для каждого объекта системы (на канальном уровне модели OSI — это аппаратный адрес сетевого адаптера, на сетевом уровне — адрес определяется протоколом сетевого уровня (например, IP-адрес). Сетевой адрес также может использоваться для идентификации объектов сети. Однако сетевой адрес достаточно просто подделывается и поэтому использовать его в качестве единственного средства идентификации объектов недопустимо. В том случае, когда в вычислительной сети использует нестойкие алгоритмы идентификации удаленных объектов, то оказывается возможной типовая удаленная атака, заключающаяся в передаче по каналам связи сообщений от имени произвольного объекта или субъекта сети (т.е. подмена объекта или субъекта сети).

Подмена доверенного объекта распределенной вычислительной сети является активным воздействием (класс 1.2), совершаемым с целью нарушения конфиденциальности (класс 2.1) и целостности (класс 2.2) информации, по наступлению на атакуемом объекте определенного события (класс 3.2). Данная удаленная атака может являться как внутрисегментной (класс 5.1), так и межсегментной (класс 5.2), как с обратной связью (класс 4.1), так и без обратной связи (класс 4.2) с атакуемым объектом и осуществляется на сетевом (класс 6.3) и транспортном (класс 6.4) уровнях модели OSI.

* **Удаленная атака «ложный объект»**

Принципиальная возможность реализации данного вида удаленной атаки в вычислительных сетях также обусловлена недостаточно надежной идентификацией сетевых управляющих устройств (например, маршрутизаторов). Целью данной атаки является внедрение в сеть ложного объекта путем изменения маршрутизации пакетов, передаваемых в сети. Внедрение ложного объекта в распределенную сеть может быть реализовано навязыванием ложного маршрута, проходящего через ложный объект.

Современные глобальные сети представляют собой совокупность сегментов сети, связанных между собой через сетевые узлы. При этом маршрутом называется последовательность узлов сети, по которой данные передаются от источника к приемнику. Каждый маршрутизатор имеет специальную таблицу, называемую таблицей маршрутизации, в которой для каждого адресата указывается оптимальный маршрут. Таблицы маршрутизации существуют не только у маршрутизаторов, но и у любых хостов (узлов) в глобальной сети. Для обеспечения эффективной и оптимальной маршрутизации в распределенных ВС применяются специальные управляющие протоколы, позволяющие маршрутизаторам обмениваться информацией друг с другом (RIP (Routing Internet Protocol), OSPF (Open Shortest Path First)), уведомлять хосты о новом маршруте — ICMP (Internet Control Message Protocol), удаленно управлять маршрутизаторами (SNMP (Simple Network Management Protocol)). Эти протоколы позволяют удаленно изменять маршрутизацию в сети Интернет, то есть являются протоколами управления сетью.

Реализация данной типовой удаленной атаки заключается в несанкционированном использовании протоколов управления сетью для изменения исходных таблиц маршрутизации. В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, которой обмениваются объекты сети, и атака перейдет во вторую стадию, связанную с приемом, анализом и передачей сообщений, получаемых от дезинформированных объектов вычислительной сети.

Навязывание ложного маршрута — активное воздействие (класс 1.2), совершаемое с любой из целей из класса 2, безусловно по отношению к цели атаки (класс 3.3). Данная типовая удаленная атака может осуществляться как внутри одного сегмента (класс 5.1), так и межсегментно (класс 5.2), как с обратной связью (класс 4.1), так и без обратной связи с атакуемым объектом (класс 4.2) на транспортном (класс 6.3) и прикладном (класс 6.7) уровне модели OSI.

Получив контроль над проходящим потоком информации между объектами, ложный объект вычислительной сети может применять различные методы воздействия на перехваченную информацию, например:

1.     селекция потока информации и сохранение ее на ложном объекте (нарушение конфиденциальности);

2.     модификация информации:

·        модификация данных (нарушение целостности);

·        модификация исполняемого кода и внедрение разрушающих программных средств – программных вирусов (нарушение доступности, целостности);

3.     подмена информации (нарушение целостности).

3.6.4 Удаленная атака «отказ в обслуживании»

Одной из основных задач, возлагаемых на сетевую операционную систему, функционирующую на каждом из объектов распределенной вычислительной сети, является обеспечение надежного удаленного доступа с любого объекта сети к данному объекту. В общем случае в сети каждый субъект системы должен иметь возможность подключиться к любому  объекту сети и получить в соответствии со своими правами удаленный доступ к его ресурсам. Обычно в вычислительных сетях возможность предоставления удаленного доступа реализуется следующим образом: на объекте в сетевой операционной системе запускаются на выполнение ряд программ-серверов (например, FTP-сервер, WWW-сервер и т.п.), предоставляющих удаленный доступ к ресурсам данного объекта. Данные программы-серверы входят в состав телекоммуникационных служб предоставления удаленного доступа. Задача сервера состоит в том, чтобы постоянно ожидать получения запроса на подключение от удаленного объекта и, получив такой запрос, передать на запросивший объект ответ, в котором либо разрешить подключение, либо нет. По аналогичной схеме происходит создание виртуального канала связи, по которому обычно взаимодействуют объекты сети. В этом случае непосредственно операционная система обрабатывает приходящие извне запросы на создание виртуального канала и передает их в соответствии с идентификатором запроса (номер порта) прикладному процессу, которым является соответствующий сервер. В зависимости от различных параметров объектов вычислительной сети, основными из которых являются быстродействие ЭВМ, объем оперативной памяти и пропускная способность канала связи — количество одновременно устанавливаемых виртуальных подключений ограничено, соответственно, ограничено и число запросов, обрабатываемых в единицу времени. С этой особенностью работы вычислительных сетей связана типовая удаленная атака «Отказ в обслуживании». Реализация этой угрозы возможна, если в вычислительной сети не предусмотрено средств аутентификации (проверки подлинности) адреса отправителя. В такой вычислительной сети возможна передача с одного объекта (атакующего) на другой (атакуемый) бесконечного числа анонимных запросов на подключение от имени других объектов.

Результат применения этой удаленной атаки — нарушение на атакованном объекте работоспособности соответствующей службы предоставления удаленного доступа, то есть невозможность получения удаленного доступа с других объектов вычислительной сети — отказ в обслуживании. Одна из разновидностей этой типовой удаленной атаки заключается  в передаче с одного адреса такого количества запросов на атакуемый объект, какое позволяет трафик. В этом случае, если в системе не предусмотрены правила, ограничивающие число принимаемых запросов с одного объекта (адреса) в единицу времени, то результатом этой атаки может являться как переполнение очереди запросов и отказа одной из телекоммуникационных служб, так и полная остановка компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов. И последней, третьей разновидностью атаки «Отказ в обслуживании» является передача на атакуемый объект некорректного, специально подобранного запроса. В этом случае при наличии ошибок в удаленной системе возможно зацикливание процедуры обработки запроса, переполнение буфера с последующим зависанием системы.

Типовая удаленная атака «Отказ в обслуживании» является активным (класс 1.2) однонаправленным воздействием (класс 4.2), осуществляемым с целью нарушения работоспособности системы (класс 2.3) на транспортном (класс 6.4) и прикладном (класс 6.7) уровнях модели OSI.

### 3.2. Характеристика и механизмы реализации типовых удаленных атак

#### Понятие типовой удаленной атаки

Исследования и анализ информационной безопасности различных распределенных ВС, проводимые авторами в течение последних лет, наглядно продемонстрировали тот факт, что, независимо от используемых сетевых протоколов, топологии, инфраструктуры исследуемых распределенных ВС, механизмы реализации удаленных воздействий на РВС инвариантны по отношению к особенностям конкретной системы. Это объясняется тем, что распределенные ВС проектируются на основе одних и тех же принципов, а, следовательно, имеют практически одинаковые проблемы безопасности; Поэтому оказывается, что причины успеха удаленных атак на различные РВС одинаковы (глава 5). Таким образом, появляется возможность ввести понятие типовой удаленной атаки. *Типовая удаленная атака*- это удаленное информационное разрушающее воздействие, программно осуществляемое по каналам связи и характерное для любой распределенной ВС. Введение этого понятия в совокупности с описанием механизмов реализации типовых УА позволяет предложить методику исследования безопасности, инвариантную по отношению к виду распределенной ВС. Методика заключается в последовательном осуществлении всех типовых удаленных воздействий в соответствии с предложенным далее их описанием и характеристиками. При этом основным элементом исследования безопасности РВС является анализ сетевого трафика (п. 3.2.1). Как пояснение последнего утверждения рассмотрим следующую аналогию: отладчик - основное средство для хакера, соответственно анализатор сетевого трафика - основное средство для сетевого хакера. Анализатор сетевого трафика по своей сути является сетевым отладчиком. Итак, в качестве методики исследования информационной безопасности распределенной ВС предлагается выполнение ряда тестовых задач, оценивающих защищенность системы по отношению к типовым удаленным воздействиям.

Рассмотрим в следующих пунктах типовые удаленные атаки и механизмы их реализации.

#### 3.2.1. Анализ сетевого трафика

Как уже отмечалось, основной особенностью распределенной ВС является то, что ее объекты распределены в пространстве и связь между ними физически осуществляется по сетевым соединениям и программно - при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами РВС, передаются по сетевым соединениям в виде пакетов обмена. Эта особенность привела к появлению специфичного для распределенных ВС типового удаленного воздействия, заключающегося в прослушивании канала связи. Назовем данное типовое удаленное воздействие *анализом сетевого трафика* (или, сокращенно, сетевым анализом).

Анализ сетевого трафика позволяет, во-первых, изучить логику работы распределенной ВС, то есть получить взаимно однозначное соответствие событий, происходящих в системе, и команд, пересылаемых друг другу ее объектами, в момент появления этих событий (если проводить дальнейшую аналогию с инструментарием хакера, то анализ трафика в этом случае заменяет и трассировщик). Это достигается путем перехвата и анализа пакетов обмена на канальном уровне. Знание логики работы распределенной ВС позволяет на практике моделировать и осуществлять типовые удаленные атаки, рассмотренные в следующих пунктах на примере конкретных распределенных ВС.

Во-вторых, анализ сетевого трафика позволяет перехватить поток данных, которыми обмениваются объекты распределенной ВС. Таким образом, удаленная атака данного типа заключается в получении на удаленном объекте несанкционированного доступа к информации, которой обмениваются два сетевых абонента. Отметим, что при этом отсутствует возможность модификации трафика и сам анализ возможен только внутри одного сегмента сети. Примером перехваченной при помощи данной типовой удаленной атаки информации могут служить имя и пароль пользователя, пересылаемые в незашифрованном виде по сети (п. 4.1).

По характеру воздействия анализ сетевого трафика является пассивным воздействием (класс 1.1). Осуществление данной атаки без обратной связи (класс 4.2) ведет к нарушению конфиденциальности информации (класс 2.1) внутри одного сегмента сети (класс 5.1) на канальном уровне OSI (класс 6.2). При этом начало осуществления атаки безусловно по отношению к цели атаки (класс 3.3).

#### 3.2.2. Подмена доверенного объекта или субъекта распределенной ВС

Одной из проблем безопасности распределенной ВС является недостаточная идентификация и аутентификация ее удаленных друг от друга объектов. Основная трудность заключается в осуществлении однозначной идентификации сообщений, передаваемых между субъектами и объектами взаимодействия. Обычно в распределенных ВС эта проблема решается следующим образом: в процессе создания виртуального канала объекты РВС обмениваются определенной информацией, уникально идентифицирующей данный канал. Такой обмен обычно называется "рукопожатием" (handshake). Однако, отметим, что не всегда для связи двух удаленных объектов в РВС создается виртуальный канал. Практика показывает, что зачастую, особенно для служебных сообщений (!?) (например, от маршрутизаторов) используется передача одиночных сообщений, не требующих подтверждения.

Как известно, для адресации сообщений в распределенных ВС используется сетевой адрес, который уникален для каждого объекта системы (на канальном уровне модели OSI - это аппаратный адрес сетевого адаптера, на сетевом уровне - адрес определяется в зависимости от используемого протокола сетевого уровня (например, IP-адрес). Сетевой адрес также может использоваться для идентификации объектов распределенной ВС. Однако сетевой адрес достаточно просто подделывается и поэтому использовать его в качестве единственного средства идентификации объектов недопустимо.

В том случае, когда распределенная ВС использует нестойкие алгоритмы идентификации удаленных объектов, то оказывается возможной типовая удаленная атака, заключающаяся в передаче по каналам связи сообщений от имени произвольного объекта или субъекта РВС. При этом существуют две разновидности данной типовой удаленной атаки:

* атака при установленном виртуальном канале,
* атака без установленного виртуального канала.

В случае установленного виртуального соединения атака будет заключаться в присвоении прав доверенного субъекта взаимодействия, легально подключившегося к объекту системы, что позволит атакующему вести сеанс работы с объектом распределенной системы от имени доверенного субъекта. Реализация удаленных атак данного типа обычно состоит в передаче пакетов обмена с атакующего объекта на цель атаки от имени доверенного субъекта взаимодействия (при этом переданные сообщения будут восприняты системой как корректные). Для осуществления атаки данного типа необходимо преодолеть систему идентификации и аутентификации сообщений, которая, в принципе, может использовать контрольную сумму, вычисляемую с помощью открытого ключа, динамически выработанного при установлении канала, случайные многобитные счетчики пакетов и сетевые адреса станций. Однако на практике, например, в ОС Novell NetWare 3.12-4.1 для идентификации пакетов обмена используются два 8-битных счетчика - номер канала и номер пакета [9]; в протоколе TCP для идентификации используются два 32-битных счетчика. Пример удаленной атаки на сеть Internet данного типа описан в п. 4.5.2.

Как было замечено выше, для служебных сообщений в распределенных ВС часто используется передача одиночных сообщений, не требующих подтверждения, то есть не требуется создание виртуального соединения. Атака без установленного виртуального соединения заключается в передаче служебных сообщений от имени сетевых управляющих устройств, например, от имени маршрутизаторов.

Очевидно, что в этом случае для идентификации пакетов возможно лишь использование статических ключей, определенных заранее, что довольно неудобно и требует сложной системы управления ключами. Однако, при отказе от такой системы идентификация пакетов без установленного виртуального канала будет возможна лишь по сетевому адресу отправителя, который легко подделать.

Посылка ложных управляющих сообщений может привести к серьезным нарушениям работы распределенной ВС (например, к изменению ее конфигурации). Рассмотренная в п. 3.2.3.1 типовая удаленная атака, использующая навязывание ложного маршрута, основана на описанной идее.

Подмена доверенного объекта РВС является активным воздействием (класс 1.2), совершаемым с целью нарушения конфиденциальности (класс 2.1) и целостности (класс 2.2) информации, по наступлению на атакуемом объекте определенного события (класс 3.2). Данная удаленная атака может являться как внутрисегментной (класс 5.1), так и межсегментной (класс 5.2), как с обратной связью (класс 4.1), так и без обратной связи (класс 4.2) с атакуемым объектом и осуществляется на сетевом (класс 6.3) и транспортном (класс 6.4) уровнях модели OSI.

#### 3.2.3. Ложный объект распределенной ВС

В том случае, если в распределенной ВС недостаточно надежно решены проблемы идентификации сетевых управляющих устройств (например, маршрутизаторов), возникающие при взаимодействии последних с объектами системы, то подобная распределенная система может подвергнуться типовой удаленной атаке, связанной с изменением маршрутизации и внедрением в систему ложного объекта. В том случае, если инфраструктура сети такова, что для взаимодействия объектов необходимо использование алгоритмов удаленного поиска (п. 3.2.3.2), то это также позволяет внедрить в систему ложный объект. Итак, существуют две принципиально разные причины, обуславливающие появление типовой удаленной атаки "Ложный объект РВС" .

#### 3.2.3.1. Внедрение в распределенную ВС ложного объекта путем навязывания ложного маршрута

Современные глобальные сети представляют собой совокупность сегментов сети, связанных между собой через сетевые узлы. При этом маршрутом называется последовательность узлов сети, по которой данные передаются от источника к приемнику. Каждый маршрутизатор имеет специальную таблицу, называемую таблицей маршрутизации, в которой для каждого адресата указывается оптимальный маршрут. Отметим, что таблицы маршрутизации существуют не только у маршрутизаторов, но и у любых хостов в глобальной сети. Для обеспечения эффективной и оптимальной маршрутизации в распределенных ВС применяются специальные управляющие протоколы, позволяющие маршрутизаторам обмениваться информацией друг с другом (RIP (Routing Internet Protocol), OSPF (Open Shortest Path First)), уведомлять хосты о новом маршруте - ICMP (Internet Control Message Protocol), удаленно управлять маршрутизаторами (SNMP (Simple Network Management Protocol)). Важно отметить, что все описанные выше протоколы позволяют удаленно изменять маршрутизацию в сети Internet, то есть являются протоколами управления сетью.

Поэтому абсолютно очевидно, что маршрутизация в глобальных сетях играет важнейшую роль и, как следствие этого, может подвергаться атаке. Основная цель атаки, связанной с навязыванием ложного маршрута, состоит в том, чтобы изменить исходную маршрутизацию на объекте распределенной ВС так, чтобы новый маршрут проходил через ложный объект - хост атакующего.

Реализация данной типовой удаленной атаки состоит в несанкционированном использовании протоколов управления сетью для изменения исходных таблиц маршрутизации.

Для изменения маршрутизации атакующему необходимо послать по сети определенные данными протоколами управления сетью специальные служебные сообщения от имени сетевых управляющих устройств (напри-мер, маршрутизаторов). В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, которой обмениваются два объекта распределенной ВС, и атака перейдет во вторую стадию, связанную с приемом, анализом и передачей сообщений, получаемых от дезинформированных объектов РВС. Методы воздействия на перехваченную информацию приведены в п. 3.2.3.3. Пример атаки данного типа в сети Internet рассмотрен в п. 4.4.

Навязывание объекту РВС ложного маршрута - активное воздействие (класс 1.2), совершаемое с любой из целей из класса 2, безусловно по отношению к цели атаки (класс 3.3). Данная типовая удаленная атака может осуществляться как внутри одного сегмента (класс 5.1), так и межсегментно (класс 5.2), как с обратной связью (класс 4.1), так и без обратной связи с атакуемым объектом (класс 4.2) на транспортном (класс 6.3) и прикладном (класс 6.7) уровне модели OSI.

#### 3.2.3.2. Внедрение в распределенную ВС ложного объекта путем использования недостатков алгоритмов удаленного поиска

В распределенной ВС часто оказывается, что ее удаленные объекты изначально не имеют достаточно информации, необходимой для адресации сообщений. Обычно такой информацией являются аппаратные (адрес сетевого адаптера) и логические (IP-адрес, например) адреса объектов РВС. Для получения подобной информации в распределенных ВС используются различные *алгоритмы удаленного поиска*, заключающиеся в передаче по сети специального вида поисковых запросов, и в ожидании ответов на запрос с искомой информацией. После получения ответа на запрос, запросивший субъект РВС обладает всеми необходимыми данными для адресации. Руководствуясь полученными из ответа сведениями об искомом объекте, запросивший субъект РВС начинает адресоваться к нему. Примером подобных запросов, на которых базируются алгоритмы удаленного поиска, могут служить SAP-запрос в ОС Novell NetWare [9], ARP- и DNS-запрос в сети Internet (п. 4.2 и 4.3).

В случае использования распределенной ВС механизмов удаленного поиска существует возможность на атакующем объекте перехватить посланный запрос и послать на него ложный ответ, где указать данные, использование которых приведет к адресации на атакующий ложный объект. В дальнейшем весь поток информации между субъектом и объектом взаимодействия будет проходить через ложный объект РВС.

Другой вариант внедрения в РВС ложного объекта использует недостатки алгоритма удаленного поиска и состоит в *периодической передаче на атакуемый объект заранее подготовленного ложного ответа* без приема поискового запроса. В самом деле, атакующему для того, чтобы послать ложный ответ, не всегда обязательно дожидаться приема запроса (он может, в принципе, не иметь подобной возможности перехвата запроса). При этом атакующий может спровоцировать атакуемый объект на передачу поискового запроса (п. 4.3.3), и тогда его ложный ответ будет немедленно иметь успех. Данная типовая удаленная атака чрезвычайно характерна для глобальных сетей, когда у атакующего из-за нахождения его в другом сегменте относительно цели атаки просто нет возможности перехватить поисковый запрос. Пример атаки данного типа на сеть Internet приведен в п. 4.3.3.

Ложный объект РВС - активное воздействие (класс 1.2), совершаемое с целью нарушения конфиденциальности (класс 2.1) и целостности информации (класс 2.2), которое может являться атакой по запросу от атакуемого объекта (класс 3.1), а также безусловной атакой (класс 3.3). Данная удаленная атака является как внутрисегментной (класс 5.1), так и межсегментной (класс 5.2), имеет обратную связь с атакуемым объектом (класс 4.1) и осуществляется на канальном (класс 6.2) и прикладном (класс 6.7) уровнях модели OSI.

#### 3.2.3.3. Использование ложного объекта для организации удаленной атаки на распределенную ВС

Получив контроль над проходящим потоком информации между объектами, ложный объект РВС может применять различные методы воздействия на перехваченную информацию. В связи с тем, что внедрение в распределенную ВС ложного объекта является целью многих удаленных атак и представляет серьезную угрозу безопасности РВС в целом, то в следующих пунктах будут подробно рассмотрены методы воздействия на информацию, перехваченную ложным объектом.

#### 3.2.3.3.1. Селекция потока информации и сохранение ее на ложном объекте РВС

Одной из атак, которую может осуществлять ложный объект РВС, является перехват передаваемой между субъектом и объектом взаимодействия информации. Важно отметить, что факт перехвата информации (фай-лов, например) возможен из-за того, что при выполнении некоторых операций над файлами (чтение, копирование и т. д.) содержимое этих файлов передается по сети, а, значит, поступает на ложный объект. Простейший способ реализации перехвата - это сохранение в файле всех получаемых ложным объектом пакетов обмена.

Тем не менее, данный способ перехвата информации оказывается недостаточно информативным. Это происходит вследствие того, что в пакетах обмена кроме полей данных существуют служебные поля, не представляющие в данном случае для атакующего непосредственного интереса. Следовательно, для того, чтобы получить непосредственно передаваемый файл, необходимо проводить на ложном объекте динамический семантический анализ потока информации для его селекции.

#### 3.2.3.3.2. Модификация информации

Одной из особенностей любой системы воздействия, построенной по принципу ложного объекта, является то, что она способна модифицировать перехваченную информацию. Следует особо отметить, что это один из способов, позволяющих *программно модифицировать поток информации между объектами РВС с другого объекта*. Ведь для реализации перехвата информации в сети необязательно атаковать распределенную ВС по схеме "ложный объект" . Эффективней будет атака, осуществляющая анализ сетевого трафика (п. 3.2.1), позволяющая получать все пакеты, проходящие по каналу связи, но, в отличие от удаленной атаки по схеме "ложный объект" , она не способна к модификации информации.

Далее рассмотрим два вида модификации информации:

* модификация передаваемых данных;
* модификация передаваемого кода.

Одной из функций, которой может обладать система воздействия, построенная по принципу "ложный объект" , является модификация передаваемых данных. В результате селекции потока перехваченной информации и его анализа система может распознавать тип передаваемых файлов (исполняемый или текстовый). Соответственно, в случае обнаружения текстового файла или файла данных появляется возможность модифицировать проходящие через ложный объект данные. Особую угрозу эта функция представляет для сетей обработки конфиденциальной информации.

Другим видом модификации может быть модификация передаваемого кода. Ложный объект, проводя семантический анализ проходящей через него информации, может выделять из потока данных исполняемый код. Известный принцип неймановской архитектуры гласит, что не существует различий между данными и командами. Следовательно, для того, чтобы определить, что передается по сети - код или данные, необходимо использовать определенные особенности, свойственные реализации сетевого обмена в конкретной распределенной ВС или некоторые особенности, присущие конкретным типам исполняемых файлов в данной локальной ОС.

Представляется возможным выделить два различных по цели вида модификации кода:

* внедрение РПС (разрушающих программных средств);
* изменение логики работы исполняемого файла.

В первом случае при внедрении РПС исполняемый файл модифицируется по вирусной технологии: к исполняемому файлу одним из известных способов дописывается тело РПС ,а также одним из известных способов изменяется точка входа так, чтобы она указывала на начало внедренного кода РПС. Описанный способ, в прин-ципе, ничем не отличается от стандартного заражения исполняемого файла вирусом, за исключением того, что ***файл оказался поражен вирусом или РПС в момент передачи его по сети!*** Такое возможно лишь при использовании системы воздействия, построенной по принципу "ложный объект" . Конкретный вид РПС, его цели и задачи в данном случае не имеют значения, но можно рассмотреть, например, вариант использования ложного объекта для создания сетевого червя - наиболее сложного на практике удаленного воздействия в сетях, или в качестве РПС использовать сетевые шпионы.

Во втором случае происходит модификация исполняемого кода с целью изменения логики его работы. Данное воздействие требует предварительного исследования работы исполняемого файла и, в случае его проведения, может принести самые неожиданные результаты. Например, при запуске на сервере (например, в ОС Novell NetWare) программы идентификации пользователей распределенной базы данных ложный объект может так модифицировать код этой программы, что появится возможность беспарольного входа с наивысшими привилегиями в базу данных.

#### 3.2.3.3.3. Подмена информации

Ложный объект позволяет не только модифицировать, но и подменять перехваченную им информацию. Если модификация информации приводит к ее частичному искажению, то подмена - к ее полному изменению.

При возникновении в сети определенного контролируемого ложным объектом события одному из участников обмена посылается заранее подготовленная дезинформация. При этом такая дезинформация в зависимости от контролируемого события может быть воспри-нята либо как исполняемый код, либо как данные. Рассмотрим пример подобного рода дезинформации.

Предположим, что ложный объект контролирует событие, которое состоит в подключении пользователя к серверу. В этом случае он ожидает, например, запуска соответствующей программы входа в систему. В случае, если эта программа находится на сервере, то при ее запуске исполняемый файл передается на рабочую станцию. Вместо того, чтобы выполнить данное действие, ложный объект передает на рабочую станцию код заранее написанной специальной программы - захватчика паролей. Эта программа выполняет визуально те же действия, что и настоящая программа входа в систему, например, запрашивая имя и пароль пользователя, после чего полученные сведения посылаются на ложный объект, а пользователю выводится сообщение об ошибке. При этом пользователь, посчитав, что он неправильно ввел пароль (пароль обычно не отображается на экране) снова запустит программу подключения к системе (на этот раз настоящую) и со второго раза получит доступ. Результат такой атаки - имя и пароль пользователя, сохраненные на ложном объекте.

#### 3.2.4. Отказ в обслуживании

Одной из основных задач, возлагаемых на сетевую ОС, функционирующую на каждом из объектов распределенной ВС, является обеспечение надежного удаленного доступа с любого объекта сети к данному объекту. В общем случае в распределенной ВС каждый субъект системы должен иметь возможность подключиться к любому объекту РВС и получить в соответствии со своими правами удаленный доступ к его ресурсам. Обычно в вычислительных сетях возможность предоставления удаленного доступа реализуется следующим образом: на объекте РВС в сетевой ОС запускаются на выполнение ряд программ-серверов (например, FTP-сервер, WWW-сервер и т.п.), предоставляющих удаленный доступ к ресурсам данного объекта. Данные программы-серверы входят в состав телекоммуникационных служб предоставления удаленного доступа. Задача сервера состоит в том, чтобы, находясь в памяти операционной системы объекта РВС, постоянно ожидать получения запроса на подключение от удаленного объекта. В случае получения подобного запроса сервер должен по возможности передать на запросивший объект ответ, в котором либо разрешить подключение, либо нет (под-ключение к серверу специально описано очень схематично, так как подробности в данный момент не имеют значения). По аналогичной схеме происходит создание виртуального канала связи, по которому обычно взаимодействуют объекты РВС. В этом случае непосредственно ядро сетевой ОС обрабатывает приходящие извне запросы на создание виртуального канала (ВК) и передает их в соответствии с идентификатором запроса (порт или сокет) прикладному процессу, которым является соответствующий сервер.

Очевидно, что сетевая операционная система способна иметь только ограниченное число открытых виртуальных соединений и отвечать лишь на ограниченное число запросов. Эти ограничения зависят от различных параметров системы в целом, основными из которых являются быстродействие ЭВМ, объем оперативной памяти и пропускная способность канала связи (чем она выше, тем больше число возможных запросов в единицу времени).

Основная проблема состоит в том, что при отсутствии статической ключевой информации в РВС идентификация запроса возможна только по адресу его отправителя. Если в распределенной ВС не предусмотрено средств аутентификации адреса отправителя, то есть инфраструктура РВС позволяет с одного объекта системы передавать на другой атакуемый объект бесконечное число анонимных запросов на подключение от имени других объектов, то в этом случае будет иметь успех типовая удаленная атака "Отказ в обслуживании" (пример подобной атаки на сеть Internet - п. 4.6). Результат применения этой удаленной атаки - нарушение на атакованном объекте работоспособности соответствующей службы предоставления удаленного доступа, то есть невозможность получения удаленного доступа с других объектов РВС - отказ в обслуживании!

Вторая разновидность этой типовой удаленной атаки состоит в передаче с одного адреса такого количества запросов на атакуемый объект, какое позволит трафик (направленный "шторм" запросов). В этом случае, если в системе не предусмотрены правила, ограничивающие число принимаемых запросов с одного объекта (адреса) в единицу времени, то результатом этой атаки может являться как переполнение очереди запросов и отказа одной из телекоммуникационных служб, так и полная остановка компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

И последней, третьей разновидностью атаки "Отказ в обслуживании" является передача на атакуемый объект некорректного, специально подобранного запроса. В этом случае при наличии ошибок в удаленной системе возможно зацикливание процедуры обработки запроса, переполнение буфера с последующим зависанием системы (пример в п. 4.7.2 - "Ping Death" ) и т. п.

Типовая удаленная атака "Отказ в обслуживании" является активным воздействием (класс 1.2), осуществляемым с целью нарушения работоспособности системы (класс 2.3), безусловно относительно цели атаки (класс 3.3). Данная УА является однонаправленным воздействием (класс 4.2), как межсегментным (класс 5.1), так и внутрисегментным (класс 5.2), осуществляемым на транспортном (класс 6.4) и прикладном (класс 6.7) уровнях модели OSI.