Лекция 15
Внешние атаки. Основные угрозы ИБ на различных уровнях сетевых протоколов. Меры борьбы с внешними атаками

15.1. Определение и виды сетевых атак

Как следует из самого названия сетевых атак, такие атаки выполняются путём проникновения злоумышленника на атакуемый компьютер через компьютерные сети, к которым имеет доступ этот компьютер.

Сетевые атаки могут быть классифицированы по цели атаки и по характеру источника атаки.

По цели сетевой атаки они разделяются на 2 различных класса:

- атаки с целью взлома системы (проникновения в систему)
- атаки, вызывающие отказ в обслуживании или DoS-атаки (Deny of Service).

По характеру источника атаки они подразделяются на:

- одиночные, выполняемые с одного компьютера
- распределённые (Distributed), выполняемые с одновременным участием нескольких, как правило значительно удаленных друг от друга (в сетевой метрике, а не просто географически) компьютеров; большинство DoS-атак являются распределёнными и, поэтому, называются DDoS-атаками.

Отметим, что достаточно серьёзные (по своим намерениям оказать атакующее воздействие на осознанно выбранный для нанесения этого воздействия компьютер (как правило выполняющий очень ответственные функции) сетевые атаки всех рассмотренных видов атакуют выбранную жертву не непосредственно с компьютеров взломщиков (злоумышленников), а с ранее взломанных ими промежуточных компьютеров или даже цепочек таких компьютеров. Делается это, в основном, по двум следующим соображениям. Во-первых, применение множества промежуточных компьютеров при выполнении сетевой атаки значительно затрудняет поиск обнаружения исходного источника атаки и обнаружение злоумышленников (чтобы привлечь их к надлежащей ответственности). А, во-вторых, промежуточный компьютер, находящийся в менее защищённой от атакуемого компьютера части сети (по сравнению с частью сети взломщика) может быть удобным “плацдармом” для сбора дополнительной информации об атакуемом компьютере и непосредственного выполнения атакующего воздействия.

15.2. Стадии развития сетевой атаки по взлому системы защиты компьютера

Сетевая атака по взлому системы защиты КСС включает 3 основные стадии: подготовительная (или разведывающая), основная и завершающая.

На *подготовительной стадии* выполняются действия, обеспечивающие возможность выполнения основной стадии. На этой стадии может “завоёвываться” цепочка “плацдармов”, используемых для проведения с них атаки на целевой компьютер. При этом “завоевание каждого плацдарма” может включать все 3 рассматриваемых стадии.

Разведывательные действия, предшествующие взлому системы защиты конкретного компьютера, могут включать

- *Сканирование портов атакуемого компьютера*, состоящее в последовательных попытках поочередного установления соединения с портами всех сетевых служб (протоколов прикладного уровня), работающих над протоколом TCP. Для большинства протоколов прикладного уровня при попытке установления соединения клиенту “на автомате” возвращается пакет banner (заголовок), содержащий сведения о типе и номере версии демона этого протокола и, возможно, некоторая дополнительная “заголовочная” информация. Для некоторых протоколов заголовочная информация по умолчанию не передаётся, но может быть дополнительно запрошена. Так, например, для протокола HTTP информация о заголовке ресурса может быть получена по запросу HEAD. Результатом сканирования сетевых портов компьютера является перечень его активных портов с указанием для каждого из них обслуживающих этот порт демонов и номеров их версий. По указанному перечню на основе специальной базы известных уязвимостей различных версий различных демонов могут быть найдены все имеющие место сетевые уязвимости сканируемого компьютера.
- *Получение дополнительной информации* об атакуемом компьютере. Если среди найденных уязвимостей компьютера нет такой, которая сразу бы позволила злоумышленнику внедрить на этот компьютер требуемый вредоносный код, работающий с правами требуемого пользователя (обычно - суперпользователя root), то злоумышленник может попытаться получить дополнительную информацию об атакуемом компьютере воспользовавшись имеющимися уязвимостями для “вспомогательных” атак с целью запуска на этом компьютере программ (от лица хоть какого-то легального пользователя), позволяющих получить информацию из оперативной памяти компьютера, его файловой системы

и внешних устройств, которая может оказаться полезной для поиска дополнительных уязвимостей компьютера “изнутри” этого компьютера.

- *Прослушивание трафика атакуемого компьютера.* Для реализации этой возможности может быть предварительно взломан какой-либо из компьютеров, находящийся в одном сетевом сегменте с атакуемым, с установкой на этом компьютере сниффера – программы, считывающей и анализирующей все передаваемые через сегмент пакеты с целью возможного перехвата логинов и паролей пользователей атакуемого и, возможно, других компьютеров. Другой способ прослушивания трафика атакуемого компьютера может быть применён и во внешних по отношению к включающему этот компьютер сегменту сетях. Этот способ базируется на возможности зеркалирования трафика порта маршрутизатора, через который поступают пакеты от атакуемого компьютера и направления зеркальной копии этого трафика для дальнейшего анализа на оснащённый специальным программным обеспечением компьютер, возможно имеющий не связанную с прослушиванием основную функциональность. Однако реализация такого способа без участия системных администраторов используемых в этой схеме маршрутизаторов и компьютеров как правило невозможна. А сложности привлечения (подкупа) сетевых администраторов тем выше, чем крупнее интернет-оператор (провайдер), маршрутизаторами которого “заведует” возможный субъект подкупа. И это обусловлено целым рядом не рассматриваемых здесь факторов. Поэтому подключение к интернету через крупных интернет-операторов снижает вероятность реализации рассмотренного способа прослушивания.
- *“Добыча” пароля организационными методами*. И основным из таких методов является подкуп системных администраторов атакуемого компьютера (КСС) или других её пользователей. Известно, что большинство крупнейших (по объёму похищенных средств) атак на банковские системы было выполнено не без использования таких методов.

  Отметим также такое распространённое в настоящее время явление, как многочисленные утечки персональных данных клиентов ряда банков, предоставляющие взломщикам информацию, упрощающую взлом ими личных кабинетов этих клиентов в информационных системах банков.

Основная стадия атаки начинается после получения на разведывательной стадии всей информации, необходимой для реализации атаки. Эта стадия начинается атакующего воздействия, внедряющего в атакуемый компьютер программный код, требуемый для реализации запланированной атаки, и активации (запуска) этого кода. В зависимости от задачи, поставленной организатором сетевой атаки, запущенный программный код может выполнить одноразовое воздействие на объект атаки или начать работу в режиме агента, выполняющего определённые действия, требуемые организатору атаки, периодически и/или при свершении в атакованной системе определённых событий. В последнем случае предпринимаются различные меры, затрудняющие обнаружение внедрённого агента.

Завершающая стадия атаки выполняется сразу после внедрения и активации атакующего кода (при этом внедрённый агент может продолжать свою работу). Её задачей является “заметание” следов атаки. Поскольку в различных системных журналах (называемых также логами - log) фиксируются различные события, происходящие в системе (события различного типа протоколируются в разных логах), при “заметании” следов выполняется “зачистка” логов путём удаления из них записей о всех событиях, связанных с атакующими действиями. В качестве примера лога, содержимое которого требуется “зачищать” укажем файл **`/var/log/wtmp`** систем UNIX, в котором фиксируется информация об установлении и завершении терминальных соединений (выполняемых как с локальных, так и с удаленных терминалов), включающая сведения о логине пользователя, выполнившего соединение, времени установления или разрыва соединения и о терминале, с которого выполнено соединение. При этом для удалённого терминала фиксируются сведения об IP-адресе компьютера, с которого выполнялось соединение. Эта информация может быть использована для обнаружения как самого факта атаки (терминальное соединение привилегированного пользователя с неизвестного компьютера, возможно, во внеурочное время), так и времени её выполнения а также компьютера с которого произошла атака. Очевидно, что при использовании “плацдармов” определяется лишь последний в цепочке посредников атаки компьютер. И очевидно, что для “заметания” следов атаки эта информация должна быть удалена из указанного файла. При этом, если в ходе атаки был внедрён постоянно работающий агент, он может продолжать работу и после “заметания” её следов.

15.3. Основные виды уязвимостей, присущих различным уровням сетевых протоколов

Основными видами уязвимостей, проявляющихся на физическом и канальном уровнях являются возможность прослушивания трафика и возможность осуществления DoS атак “глушения” каналов.

Возможность прослушивания трафика (в том числе пакетов авторизации, содержащих логин и пароль некоторого пользователя) обеспечивает получение информации, необходимой для проведения сетевых атак, основанных на знании логина и пароля какого-либо из пользователей атакуемого компьютера. Кроме того, эта возможность обеспечивает доступ к любой другой конфиденциальной информации, передаваемой через сетевые каналы в незашифрованном виде. Эта возможность может быть реализована как минимум тремя способами. Первый способ реализуется на канальном уровне и применим лишь для прослушивания трафика шинных Ethernet-сегментов. Как упоминалось в главе два сетевая карта Ethernet может быть программно переведена в режим прослушивания (считывания) абсолютно всех пакетов, передаваемых через сегмент. Такой перевод и организацию последующего прослушивания трафика и “извлечения” из него различной информации быть сделано, например, с помощью программ, называемых *снифферами* (от *to sniff* – нюхать, вынюхивать), выполняющими перехват и анализ содержания пакетов. Наиболее известным представителем программ этого класса является бесплатная программа Wireshark, обеспечивающая анализ трафика различных сетей канального уровня (Ethernet, FDDI, PPP и других) в режиме реального времени.

Второй способ прослушивания трафика основан на применении специального оборудования, устанавливаемого в непосредственной близости от сетевых кабелей, основанных на передаче электрического сигнала, и позволяющего воспроизводить передаваемый электрический сигнал на основе магнитного поля, возникающего при обработке сигнала. По создаваемым угрозам безопасности этот способ прослушивания трафика ничем не отличается от рассмотренного выше. Но такой способ прослушивания проще обнаружить путём регулярного осмотра кабельных систем. Кроме того, такой способ прослушивания можно полностью исключить путём использования волоконно-оптических кабелей взамен проводных электрических.

Третий способ может быть применён для прослушивания трафика сетей, использующих радиоканалы передачи данных. Радиосигнал доступен для просушивания

абсолютно всем. Поэтому, естественно, для исключения возможности “понимания” этого сигнала он шифруется. Но используемая система шифрования может быть недостаточно надёжна и подвергнуться взлому.

Возможность осуществления DoS атаки путем “глушения” канала может быть реализована для каналов, основанных на передаче электромагнитного сигнала: радиоканалов и электрических кабелей (волоконно-оптические каналы совершенно не подвержены таким атакам). Глушение радиоканала может быть выполнено мощным передатчиком, работающим на той же частоте, что и используемая сетевым приёмо-передатчиком. Для кабельных каналов “глушение” (искажение передаваемого сигнала” до неузнаваемости) может быть выполнено путём воздействия стороннего электромагнитного поля. Способом создания такого стороннего поля для электрических сетевых кабелей может быть, например, прокладка параллельного сетевому кабелю кабеля электропитания переменного тока на небольшом (примерно до 5 см.) расстоянии от сетевого кабеля. Это вызовет помехи в передаваемом по сетевому кабелю сигнале. Другим простым, но более “дальнобойным” способом, является установка (возможно, в некотором отдалении и вне помещения с сетевым кабелем) постоянно и сильно искрящего устройства, такого, например, как работающего электрогенератора (например, автомобильного) с неисправными токосъёмными щётками. И, конечно же, сильное электромагнитное поле может создаваться специально созданными для этого устройствами, осознанно не уточняемыми в этой книге. Упомянём лишь о существовании электромагнитного оружия, способного на значительных расстояниях (десятки и сотни метров) выводить из строя практически любое радиоэлектронное и компьютерное оборудование путём наведения токов высокого напряжения.

Основные виды уязвимостей, характерные для IP-уровня включают: возможность IP-спуфинга, возможность перехвата трафика, и возможность DoS и DDos атак на маршрутизаторы, возможность DoS и DDos атак на произвольные устройства IP-сети и др.

IP-spoofing (*spoofing* - мистификация) - это подмена в IP-пакете правильного IP-адреса отправителя на другой IP-адрес. Он может быть выполнен непосредственно на компьютере отправителя. Применяется в ряде сетевых атак, например, для того, чтобы вызвать ответный пакет на нужный адрес, как это делается в рассматриваемой ниже атаке smurf. Защита от этой угрозы может основываться на проверке правильности сопоставленного истинному адресу отправителя его MAC-адреса, но для этого получатель пакета должен знать этот MAC-адрес, что возможно далеко не всегда.

Возможность перехвата трафика на IP-уровне основывается на возможности зеркалирования трафика портов. Мы уже рассматривали эту возможность, способы её реализации, а также возможного снижения вероятности такой реализации при рассмотрении разведывательной стадии атаки.

DoS и DDos атаки на маршрутизатор могут быть реализованы путём "забрасывания" маршрутизатора чрезмерно большим числом пакетов маленького размера, выполняемого с одного или нескольких компьютеров для DoS и DDos атак соответственно. Маршрутизатор затрачивает на обработку любого пакета некоторое фиксированное время обработки плюс время отправки пакета. Поэтому максимальная нагрузка на процессор маршрутизатора со стороны определённого его порта (порта, ведущего во внешние сети, в которых обычно находятся источники атаки) при фиксированной и часто не очень большой пропускной способности этого канала может быть создана путём максимально возможного увеличения числа поступающих из этого порта пакетов. Это может быть достигнуто путём максимального уменьшения размеров этих пакетов. Созданная перегрузка способна вызвать полный отказ в способности маршрутизатора обрабатывать обычные (не атакующие) IP-пакеты.

Примером DoS и DDos атак на произвольные устройства IP-сети является известная атака smurf (*smurf* – разбивание большой суммы денег на части с целью "отмывания" этой суммы), состоящая в передаче в сеть отправляемых одним или несколькими компьютерами широковещательных ICMP запросов от имени атакуемого компьютера. Все компьютеры, принявшие такие широковещательные запросы, направляют ответы атакуемому компьютеру, что приводит к перегрузке каналов связи к этому компьютеру, а, возможно, и к включающей этот компьютер подсети.

Основными уязвимостями транспортного уровня являются возможность перехвата TCP-соединений и возможность DoS атак портов прикладных служб.

Перехват TCP-соединений может быть реализован, например, с использованием функции зеркалирования портов маршрутизатора (но может осуществляться и дополнительным ПО, установленным на маршрутизатор администратором-инсайдером). Пример того, как с помощью перехвата TCP-соединений реализуется блокировка доступа к веб-страницам, указанных в неком реестре запрещённых страниц, приведён нами при рассмотрении в главе 3 функции зеркалирования портов. Если известны IP-адрес и номер порта одной из сторон соединения, то функции "перехватывающей программы только

упростятся. Методами перехвата TCP-соединений могут быть реализованы некоторые сетевые атаки.

Вопросы, связанные с привлечением для реализации подобных действий администраторов маршрутизаторов рассмотрены нами выше в настоящем пункте текущей главы при рассмотрении подготовительных (разведывательных) действий по проведению сетевой атаки.

Защититься от перехвата TCP соединений можно путём использования криптографических методов защиты. При использовании защищённого транспортного протокола TLS (бывшего SSL) TCP-сообщения, адресованные интересующей взломщика стороне соединения в принципе, могут быть перехвачены, поскольку требуемая "перехватчику" адресная информация о сторонах соединения, содержащаяся в TCP-заголовках, указанными протоколами не шифруется. Но для "разумных ответов" на перехваченные пакеты необходимо "понимать" их содержимое. А это невозможно ввиду зашифрованности этого содержимого. Предотвратить возможность перехвата TCP-сообщений можно путём шифрования информации на IP-уровне. Для IPv4 такое шифрование обеспечивается протоколом IPSec, в протоколе IPv6 требуемая криптографическая защита реализуется с использованием дополнительных заголовков Encapsulation пакетов IPv6. Поскольку при шифровании содержимого IP-пакетов транспортные сообщения шифруются вместе с их заголовками, становится недоступным требуемое для перехвата TCP-сообщения содержимое его заголовка.

DoS атаки портов прикладных служб, в частности, могут быть основаны на рассмотренных в главе 5 TCP Sync атаках. И хотя современные реализации протокола TCP делают Sync атаки невозможными, не исключена вероятность того, что хакеры найдут или уже нашли другие способы создания чрезмерной нагрузки на порты произвольных сетевых служб.

Множество уязвимостей, присущих прикладному уровню неизмеримо шире состава уязвимостей, присущих каждому из предыдущих уровней, что естественно объясняется большим количеством и разнообразием этих протоколов. В число этих уязвимостей входят, в частности, возможность компрометации службы DNS, возможность перехвата паролей для ряда прикладных протоколов, возможные уязвимости CGI-скриптов и работающих на стороне веб-клиента программ, возможные новые уязвимости

в программах демонов и клиентов разнообразных сетевых служб, возможные уязвимости в прикладных программах пользователей и некоторые другие виды уязвимостей.

Компрометация службы DNS (или DNS-spoofing) может быть выполнена методом перехвата TCP соединения. В результате запрос, направленный некоторому DNS-серверу может быть перехвачен и направлен, например, хакерскому DNS серверу, сообщающему клиенту вместо запрошенных ими IP-адресов сайтов производителей программного обеспечения IP-адреса хакерских версий этих сайтов, “нашпигованных” заражёнными вирусами и/или содержащими троянский код версиями программ этого производителя. Эта цепочка обычно укорачивается и не содержит хакерского DNS-сервера: перехватывающая TCP соединение программа вполне может самостоятельно определить, что указанное в запросе имя является именем сайта производителя ПО и возвратить в качестве ответа IP-адрес хакерской версии этого сайта.

Долгое время единственным методом борьбы с этой уязвимостью была так называемая двойная DNS-проверка. Суть её состоит в том, что при получении запрашиваемого IP-адреса выполняется ещё один запрос к службе DNS на обратное преобразование IP-адреса в доменное имя. Если результат этого запроса совпадает с исходным именем, указанным в исходном DNS-запросе, считается что служба DNS не скомпрометирована. Это мотивируется ничтожно малой вероятностью перехвата обоих выполняемых при двойной проверке TCP соединений.

Однако практически все сетевые приложения обращаются к службе DNS без двойной проверки. Поэтому был придуман способ, обеспечивающий выполнение двойных DNS-проверок. Этот способ основан на специальном “заворачивании” программ сетевых приложений в специальные программы wrapper’ы (рэпперы) или обёртки, (wrapper – обёртка , “пропускающими” через себя все сообщения, пересылаемые между приложениями и модулем TCP. Требуемое “заворачивание” выполняется при инсталляции и конфигурировании программы-рэппера. Такой рэппер при пропуске через себя запросов к службе DNS может отслеживать их и самостоятельно выполнять 2-й запрос двойной DNS-проверки и обнаруживать возможный факт компрометации.

Отметим, что программы-рэпперы могут быть специализированными, обеспечивающими возможность “обёртывания” лишь вполне определённых прикладных программ (например, почтового демона sendmail), или универсальными, такими как

широко известная программа TCP wrapper, пропускающая через себя все сообщения, пересылаемые между протокольным модулем TCP и программами всех приложений и контролирующая допустимость передачи каждого из сообщений.

Хотя описанное выше решение по обнаружению фактов компрометации службы DNS методами перехвата TCP-соединений было найдено, служба обладала и некоторыми другими уязвимостями, например с возможностью реализации атаки DNS cache poisoning, изменяющей данные в кэше DNS-сервера, также приводящей к компрометации службы DNS. Поэтому к 2011 году был разработан протокол DNSSEC, представляющий собой развитие традиционных протоколов DNS средствами, позволяющими исключить подмену передаваемых IP-адресов. DNSSEC является технологией, обеспечивающей защиту от таких подмен с помощью цифрового "подписывания" данных (криптографической цифровой подписью), которое подтверждает остоверность этих данных. При этом сами данные пересылаются в незашифрованном виде, что позволило обеспечить совместимость DNSSEC с существовавшими к моменту разработки незащищенными протоколами DNS. Отметим, что стойкость ко взломам используемой в DNSSEC криптографической системы шифрования цифровых подписей оказалась столь высокой, что используемые ключи шифрования не менялись с момента создания протокола DNSSEC до ноября 2018 года, когда впервые за историю существования DNSSEC состоялась массовая замена ключей, используемых этой службой для шифрования цифровых подписей.

Возможность перехвата логинов и паролей пользователей ряда прикладных протоколов, таких как TELNET, FTP и ряда других неоднократно упоминалась при рассмотрении таких протоколов. Опасность такого перехвата вполне очевидна. Также очевидно, что избежать этой возможности можно лишь отказавшись от использования упомянутых небезопасных протоколов и перейдя на использование их защищённых аналогов: SSH, SFTP и пр.

Возможные уязвимости CGI-скриптов и работающих на стороне веб-клиента программ, рассмотрение которых выходит за рамки нашего курса.

Возможные новые уязвимости в программах демонов и клиентов разнообразных сетевых служб. Как известно, после обнаружения уязвимости некоторого типа, присущей конкретной программе или некоторому множеству программ, производители программ, обладающих этой уязвимостью находят способ такого изменения уязвимых фрагментов этих программ, при котором обнаруженная уязвимость устраняется. Для оперативного

внесения требуемых изменений во всех инсталляциях уязвимых программ разрабатываются программы патчей (заплаток), устраняющих уязвимость во всех поддерживаемых производителем версиях программ прямо на компьютерах их пользователей. Соответствующим образом изменяются и распространяемые производителем дистрибутивы этих программ. Новые же версии программ уже при их создании не содержат рассматриваемых уязвимостей. Тем не менее, не исключено, что в процессе эксплуатации тех или иных программ, ранее считавшихся неуязвимыми, хакерами будут найдены некие приёмы, позволяющие получить возможность создания не предусмотренных при создании этих программ точек “левого” входа в эти программы, выполняемого без проверки полномочности этого входа. Такие новые уязвимости могут быть присущи как вполне определённым программам, так и достаточно широкому классу программ. Отметим, что по количеству обнаруженных в разные годы уязвимостей явными лидерами является почтовый демон sendmail и почтовая служба в целом. Поэтому при появлении атак неизвестного типа из возможных версий по способам реализации этих атак в первую очередь рекомендуется рассмотреть версии, связанные с функционированием службы электронной почты.

Возможные уязвимости в прикладных программах пользователей могут быть связаны, например, с тем, что разработчики этих программ не знакомы со всеми потенциально опасными приёмами программирования и использовали при разработке программ какие-либо из таких приёмов. Более серьёзную угрозу представляет случай сознательного включения разработчиком в создаваемую им программу специальных “закладок” - кода, позволяющего обойти систему защиты КСС. Поэтому прикладные программы, применяемые в КСС, к которым предъявляются высокие требования информационной безопасности, должны проходить специальную проверку их информационной безопасности. Если такая проверка выполняется специальными уполномоченными органами, то она называется сертификацией информационной безопасности программ.

1.5.4. Методы борьбы с внешними атаками

Комплекс мер по борьбе с внешними атаками включает как обязательную составную часть все меры, применяемые при борьбе с внутренними атаками. Кроме того предпринимается ряд дополнительных мер, включающих:

- возможное повышение требований к используемому оборудованию и программному

обеспечению (ПО),

-применение средств криптозащиты не только хранимой, но и для передаваемой через сеть информации;

- обеспечение максимально возможной изоляции компьютерных сетей организаций, их подразделений, индивидуальных пользователей и распределённых приложений от всех ненужных для их работы внешних и внутренних подсетей;

- применение систем обнаружения вторжений.

Возможное повышение требований к используемому оборудованию и ПО состоит в следующем. Для КСС, предъявляющих повышенные требования к информационной безопасности, одним из важнейших является требование наличия сертификатов ИБ для всех используемых в составе КСС аппаратных и программных средств, как обеспечивающих основную функциональность этих КСС, так и предназначенных для обеспечения ИБ КСС. Сертификация программно-аппаратных средств на их ИБ подтверждает отсутствие в этих средствах аппаратных и программных “закладок”, предназначенных для осуществления тех или иных нарушений системы ИБ КСС. Такую сертификацию осуществляют уполномоченные на её проведение органы. В частности, всё оборудование и некоторые виды ПО сетей операторов связи должны быть сертифицированы Министерством связи РФ (его уполномоченными организациями. Оборудование и ПО всех КСС работающих с конфиденциальной информацией (например, коммерческими или научными секретами) должно быть сертифицировано ФСТЭК (Федеральной службой по таможенному и экспортному контролю), средства, используемые в КСС, работающих с информацией, составляющей государственную тайну, должны быть сертифицированы ФСБ (Федеральной службой безопасности). Кроме того, все используемые средства криптографической защиты должны использовать лишь разрешённые ФСБ алгоритмы шифрования.

Применение средств криптозащиты предполагает, во-первых, шифрование конфиденциальной информации (хранящейся в памяти и/или передаваемой через сеть), содержание которой ни в коем случае не должна быть доступна злоумышленнику, и, во-вторых, надёжную взаимную аутентификацию партнёров каждого защищённого сетевого взаимодействия. Шифрование информации, передаваемой через сеть может обеспечиваться средствами защищенных сетевых протоколов и/или средствами создания защищённых каналов. Отметим, что защищённые каналы могут строиться как на применении средств криптозащиты, так и на частичном или полном исключении

возможности прослушивания каналов, например, средствами VLAN (L2 VPN) или MPLS (L3 VPN). Средства криптозащиты рассматриваются в лекции 17. Вопросы применения средств VPN для создания защищенных каналов вкратце рассматриваются в следующей лекции.

Максимально возможная изоляция компьютерных сетей организаций, их подразделений, индивидуальных пользователей и распределённых приложений от всех ненужных для их работы внешних и внутренних подсетей имеет целью предельно сузить (в идеале - до пустой) совокупность областей внешней и/или внутренней сети, из которых возможно выполнение атакующих действий на защищаемую однокомпьютерную или распределённую систему.

Изоляция объекта защиты (индивидуального компьютера или сети) от ненужного и потенциально опасного окружения может выполняться с использованием двух различных средств: межсетевых экранов (МЭ) и виртуальных частных сетей (VPN). VPN уже были рассмотрены нами ранее. МЭ и специфика используемых в них методов изоляции объекта защиты от потенциально опасного окружения рассматриваются в следующей лекции.

Системы обнаружения вторжений являются средством обнаружения факта проведения сетевой атаки и возможного её принудительного прерывания. Методы работы таких систем рассматриваются в следующей лекции.