7. ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

[информационная безопасность; компьютерные преступления; компьютерные злоупотребления; угрозы в сети; вредоносное ПО; антивирусное ПО; брандмауэры; IDS, IPS]

В связи с массовой информатизацией современного общества все большую актуальность приобретает знание нравственно-этических норм и правовых основ использования средств новых информационных технологий в повседневной практической деятельности. Наглядными примерами, иллюстрирующими необходимость защиты информации и обеспечения информационной безопасности, являются участившиеся сообщения о компьютерных взломах банков и иных организаций, росте компьютерного пиратства, распространении компьютерных вирусов.

Число компьютерных преступлений растет. Также увеличиваются масштабы компьютерных злоупотреблений. Умышленные компьютерные преступления составляют заметную часть всех преступлений. Но злоупотреблений и ошибок еще больше. Основной причиной потерь, так или иначе связанных с компьютерами, является недостаточная образованность в области безопасности. Только наличие некоторых знаний в области безопасности может прекратить инциденты и ошибки, обеспечить эффективное применение мер защиты, предотвратить преступление.

7.1. Компьютерные преступления и злоупотребления и методы противодействия им

Под *информационной безопасностью* понимается защищенность информации от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации.

Цель информационной безопасности – обезопасить ценности системы, защитить и гарантировать точность и целостность информации, минимизировать потери, если информация будет модифицирована или разрушена.

На практике важнейшими являются три аспекта информационной безопасности:

- *доступность* (возможность за разумное время получить требуемую информационную услугу);
- *целостность* (защищенность информации от разрушения и несанкционированного изменения);
- *конфиденциальность* (защита от несанкционированного прочтения).

Кроме того, использование информационных систем должно производиться в соответствии с существующим законодательством. Это положение, разумеется, применимо к любому виду деятельности, однако информационные технологии специфичны в том отношении, что развиваются исключительно быстрыми темпами. Почти всегда законодательство отстает от потребностей практики, и это создает в обществе определенную напряженность. Для информационных технологий подобное отставание законов, нормативных актов, национальных и отраслевых стандартов оказывается особенно болезненным.

Формирование режима информационной безопасности – проблема комплексная. Меры по ее решению можно подразделить на четыре уровня:

- *законодательный* (законы, нормативные акты, стандарты и т. п.);
- *административный* (действия общего характера, предпринимаемые руководством организации);
- *процедурный* (конкретные меры безопасности, имеющие дело с людьми);
- *программно-технический* (конкретные технические меры).

Различают четыре уровня защиты информации:

- *предотвращение* – доступ к информации и технологии предоставляется только для персонала, получившего допуск от собственника информации;
- *обнаружение* – обеспечивается раннее обнаружение преступлений и злоупотреблений, даже если механизмы защиты были обойдены;
- *ограничение* – уменьшается размер потерь, если преступление все-таки произошло, несмотря на меры по его предотвращению и обнаружению;
- *восстановление* – обеспечивается эффективное восстановление информации при наличии документированных и проверенных планов по восстановлению.

Если еще недавно контроль защиты информации был заботой преимущественно технических администраторов, сегодня это становится обязанностью каждого пользователя, что требует от него новых знаний и навыков. Так, эффективный контроль безопасности информации требует понимания возможностей совершения компьютерных преступлений и злоупотреблений для принятия контрмер против них.

Для защиты информации каждый пользователь ПК должен знать и осуществлять ряд необходимых мер. А именно:

1. Контролируйте доступ как к информации в компьютере, так и к прикладным программам.

2. При работе на ПК, доступ к которому имеют и другие лица, требуйте, чтобы все они выполняли процедуры входа в компьютер, и используйте это как средство для аутентификации в начале работы.

3. Используйте уникальные пароли для аутентификации каждого пользователя, работающего на том же ПК, не являющиеся комбинациями их личных данных.

Работая в Internet, всегда следует помнить, что подключение к нему, хотя и предоставляет огромные выгоды из-за доступа к колоссальному объему информации, оно же яв-

ляется опасным для сайтов с низким уровнем безопасности. Фундаментальная проблема состоит в том, что Internet при проектировании не задумывался как защищенная сеть. Как следствие – полный набор типичных проблем, связанных с обеспечением безопасности собственных информационных ресурсов:

- легкость перехвата данных и фальсификации адресов компьютеров в Internet, поскольку значительная часть его трафика – нешифрованные данные;
- многие web-сайты сконфигурированы таким образом, что предоставляют широкий доступ к себе со стороны Internet без учета возможности злоупотребления этим доступом;
- многие web-сайты не пытаются ограничить доступ к информации о своих компьютерах, которая может помочь злоумышленникам.

7.2. Источники и типы угроз в сети

С распространением интернета всё больше компаний переносило часть своей деятельности в глобальную сеть, а некоторые даже полностью организовывали деятельность в ней. Всё это и привело к появлению *кибер-преступности*. Преступники преследуют различные цели: кража конфиденциальной информации (например, данные кредитных карточек пользователей или корпоративная информация); вывод из строя инфраструктурных служб различных предприятий; *DoS* (*Denial Of Service – отказ в обслуживании*) атаки на различные публичные серверы.

Наиболее известны три типа атак на ресурс содержащие серверы Internet:

1. *Отказ в обслуживании* (DoS) – имеет место, когда сервер или сервис подвергается атаке, препятствующей доступу других пользователей сети. Атака DoS имеет множество видов:

- *DoS разрушители* (*destroyers*) пытаются уничтожить данные и программное обеспечение хоста;
- *DoS взломщики* (*crashers*) вызывают сбои на хосте и делают его недоступным для других устройств в сети;
- *DoS заполнители* (*flooders*) переполняют сеть пакетами лишая пользователей возможности установки связи с хостами.
- *Атака SYN* - в результате её происходит открытие TCP портов случайным образом. В итоге сетевое оборудование или хосты перегружаются огромным количеством ложных запросов, в результате чего пользователем отказывается открытие сеанса.
- *DDoS* (*Distributed Denial of Service*) – распределенная атака вызывающая отказ в обслуживании. В DDoS атаке применяются те же методы что и в DoS, только атака происходит одновременно со множества компьютеров.
- *DRDoS* – распределённая *рефлективная* DoS атака. Имеет место в случаях, когда злоумышленник посылает на несколько компьютеров в Internet сообщение, изменив адрес источника пакета на адрес цели. Системы, получившие этот запрос, отправляют отклики компьютеру жертвы.

2. *Разведывательные* (*reconnaissance*) атаки. Их цель – сбор информации для последующей атаки. Пример такой атаки – попытка выяснения IP-адреса сервера или номеров портов служб, работающих на сервере.

3. *Атака доступа* – её цель выкрасть конфиденциальные данные, к которым у злоумышленника нет доступа. Пример – кража корпоративных данных (информации о клиентах, финансовая отчётность и т.д.).

Одним из самых популярных из множества существующих приемов осуществления различных атак на сетевые ресурсы *выступает распространение вредоносного программного обеспечения* (*ВПО*). ВПО в общем случае представляет собой программу, тайно проникающую на компьютер, например, через электронное письмо или вместе с загружаемым с Web-сайта файлом. ВПО, как правило, нарушает работу компьютера (например, может создавать большое количество процессов, которые требуют дополнительное место в оперативной памяти и создают дополнительную нагрузку на процессор) или даже может передать информацию с компьютера создателю вредоносной программы.

Может сложиться представление, что различные угрозы могут исходить только из внешней сети, что неверно. На рисунке 7.1 показана некоторая топология сети, а также отражены некоторые из возможных ситуаций, в которых атака осуществляется из внутренней сети.

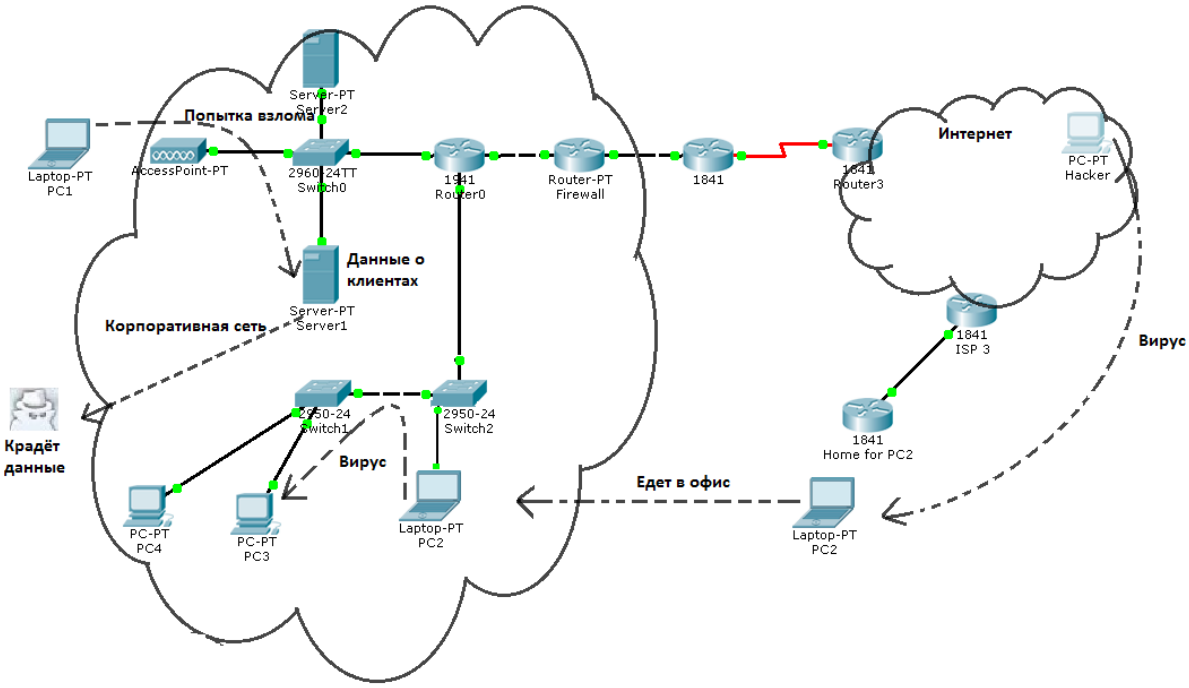

Рисунок 7.1. Возможный вариант атаки из внутренней сети

Атака из внутренней сети может реализовываться в нескольких вариантах:

- *Доступ из беспроводной сети*. Сигнал от точки доступа распространяется за пределы здания, в котором развернута сеть, и при отсутствии необходимой защиты в сеть может войти злоумышленник.
- *Инфицированный ВПО ноутбук* (или иной мобильный компьютер). Сотрудник берет с собой домой рабочий ноутбук. В его домашней сети нет брандмауэра и других средств защиты, в результате чего его домашний компьютер может оказаться зараженным ВПО.

Когда сотрудник возвращается на работу и подключается к корпоративной сети, существует риск заражения других компьютеров в этой сети.

- *Увольняемый сотрудник*. Пользователь имеет доступ к серверу компании. Он делает копию необходимых файлов и уносит их с собой.

Помимо ВПО существуют и другие средства, которые могут быть использованы для совершения атаки:

- *Сканер сети*: средство, которое посылает запросы на соединение портам различных приложений, тем самым пытаясь определить, какие службы работают на хостах.
- *Программы шпионы* (*spyware*): крадут конфиденциальную информацию или отслеживают действия пользователей на компьютере. Полученную информацию передают атакующему.
- *Регистратор нажатия клавиш на клавиатуре (keystroke logger)*: программа, которая записывает нажатия клавиш на клавиатуре. Она может записывать все нажатия, а может только те, с помощью которых вводятся данные от различных аккаунтов. Вся полученная информация передается атакующему.
- *Фишинг (Phishing)*: злоумышленник создаёт Web-сайт, внешне очень схожий с реальным Web-сайтом какой-либо компании или сервиса. Затем каким-либо образом мошенник распространяет URL, который тоже очень схож с реальным URL компании, но на самом деле ведёт на *фишинговый Web-сайт*. В итоге, некоторые невнимательные пользователи могут не заметить обмана и передать такому Web-сайту свои конфиденциальные данные.

Решением этих и множества других проблем является организация многоуровневой безопасности сети. При такой организации должен использоваться не только какой-то один программный продукт или аппаратное средство, а комплекс различных технологий и средств. Ниже будут рассмотрены средства, которые можно применить для организации многоуровневой защиты.

7.3. Обнаружение вторжений в сеть и их предотвращение

Некоторые виды атак имеют весьма сложный характер. В них даже не обязательна передача какого-либо файла или ВПО, вместо этого применяется какой-либо из множества других, более изощренных методов, например, могут использоваться уязвимости операционных систем или различных приложений. Для предотвращения сложных атак, как правило, используются два инструментальных средства.

7.3.1. Система обнаружения вторжений

Система обнаружения вторжений (Intrusion Detection System – IDS) представляет собой аппаратное или программное решение, пассивно наблюдающее за трафиком сети. Сетевой трафик не проходит непосредственно через IDS (рис.7.2). IDS следит за трафиком через сетевой интерфейс. Обнаруживая вредоносный трафик, IDS отправляет предупреждения на заранее настроенные станции.

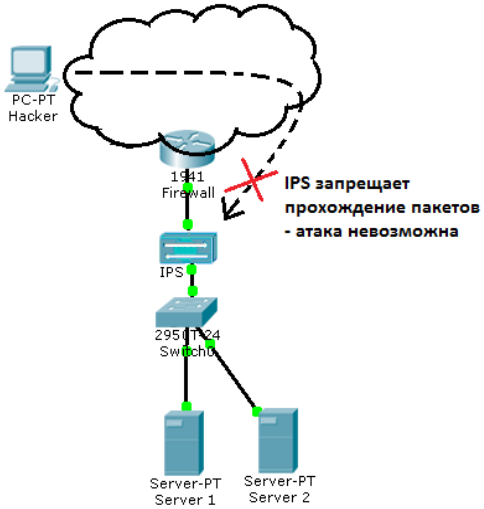

Рис.7.2. Использование IDS

IDS- предназначены для реакции на вторжение. Такие системы обнаруживают вторжение по особым сигнатурам трафика или по характеру поведения хостов. Они не препятствуют пересылке исходного трафика адресату, но позволяют отреагировать на событие. Правильно сконфигурированная IDS способна блокировать последующий трафик.

7.3.2. Система предотвращения вторжений

Система предотвращения вторжений (*Intrusion Prevention System – IPS*). Представляет собой физическое устройство или программное средство. Трафик поступает через один интерфейс IPS и выходит через другой (рис. 7.3.).

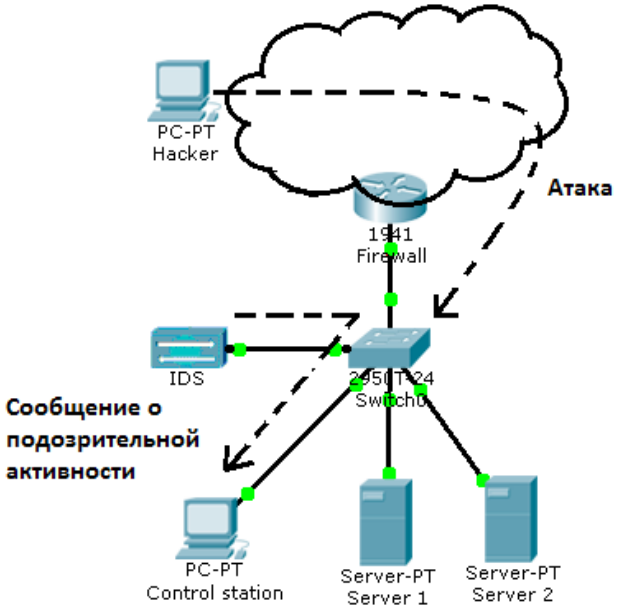

Рис.7.3. Использование IPS

Система IPS анализирует пакеты непосредственно составляющие сетевой трафик и в режиме реального времени разрешает или запрещает прохождение пакетов в сеть.

Обе рассмотренные системы реализуются в сети посредством сенсоров. Сенсором могут выступать следующие устройства:

- Маршрутизатор, поддерживающий IPS;
- специальное оборудование, которое выполняет функции IPS или IDS;
- сетевой модуль, установленный в коммутаторе, маршрутизаторе или специальных устройствах защиты.

IPS, в отличие от IDS, предназначена для профилактики вторжений. IPS способна блокировать все подозрительные действия в реальном времени, способна анализировать практически всю информацию со второго по седьмой уровень модели OSI, позволяет автоматически отсылать оповещения о вторжениях на управляющие станции, блокировать как исходный, так и последующий вредоносный трафик.

Чаще всего IPS организуется совместно с брандмауэром. Брандмауэр не проверяет пакеты полностью в отличие от IPS. Брандмауэр отбрасывает большинство запрещённых пакетов, но может пропустить некоторые вредоносные. IPS требуется анализировать меньше пакетов, но проверять их полностью, таким образом, IPS способна блокировать атаки, которые не может предотвратить брандмауэр.