Занятие 53: Основные понятия информационной безопасности

Основные понятия и определения **1**
Основные требования к безопасности системы 1
Целостность и доступность системы 3
Угроза, атака, риск 4
Классификация компьютерных угроз 4
Основные типы умышленных угроз **6**
Незаконное проникновение в систему 6
Нелегальные действия легальных пользователей 7
«Подслушивание» внутрисетевого трафика 7
Базовые принципы политики безопасности **8**
Типы и примеры атак **9**
Атаки отказа в обслуживании 9
Перехват и перенаправление трафика 9
Некоторые приемы перехвата трафика 11
Резюме **11**
Основные требования к информационной безопасности систем . 11
Понятия угрозы, атаки, риска. Основные виды атак 12
Современные компьютерные угрозы. Трояны, черви, вирусы 12
Базовые принципы политики информационной безопасности 13

Литература

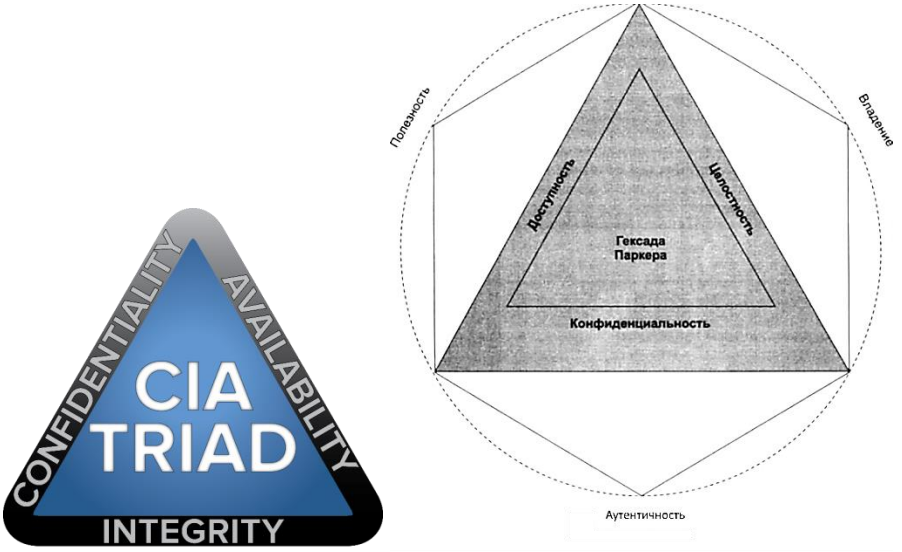
ОИ6. Олифер, В. Компьютерные сети: Учебник для вузов. 5-е изд. / В. Олифер, Н. Олифер – СПб.: Питер, 2016. – 992 с.: ил. – С. 738-770 (глава 26 «Основные понятия, концепции и принципы информационной безопасности»)

Основные понятия и определения

Основные требования к безопасности системы

Под **информационной безопасностью** понимается состояние защищенности информационной системы, включая собственно информацию и поддерживающую ее инфраструктуру.

Одной из первых и наиболее популярных по сей день моделей безопасности является модель, предложенная Зальцером (Saltzer) и Шредером (Schroeder). Авторы постулировали, что все возможные нарушения информационной безопасности всегда могут быть отнесены по меньшей мере к одной из трех групп: нарушения конфиденциальности, нарушения целостности или нарушения доступности. Эта модель получила название «триада КЦД», или «триада CIA» (по первым буквам: Confidentiality, Integrity, Availability).



Триада CIA и гексада Паркера

> Информационная система считается защищенной, если обеспечены ее **конфиденциальность, доступность и целостность**.

Указанные три требования являются основными.

> Конфиденциальность – это гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен.

Такие пользователи называются легальными, или авторизованными.

> Доступность – это гарантия того, что авторизованные пользователи всегда получат доступ к данным

И, наконец,

> Целостность – это гарантия сохранности данными правильных значений

другими словами – запрет неавторизованным пользователям каким-либо образом изменять, модифицировать, разрушать или создавать данные.

Существуют и другие модели информационной безопасности - например, гексада Паркера (см. рис.). **ГОСТ 13335-1:2006** дает определение информационной безопасности именно на основе гексады Паркера:

> **Информационная безопасность (ИБ)** это все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.

Предлагались и другие модели. Их разнообразие подтверждает общее правило: **БЕЗОПАСНОСТИ НЕ БЫВАЕТ МНОГО**.

> Требования безопасности могут меняться в зависимости от назначений информационной системы, характера используемых данных и типа возможных угроз.

Например, конфиденциальность не требуется для информации, размещаемой на Web-сервере, если вы собираетесь сделать ее доступной для широкого круга потенциальных клиентов. Однако

> требования целостности и доступности всегда остаются актуальными.

Целостность и доступность системы

> Понятия конфиденциальности, доступности и целостности могут быть определены не только по отношению к информации, но и к другим ресурсам вычислительной сети

– таким, как внешние устройства или приложения. Так, свойство конфиденциальности по отношению к устройству печати можно интерпретировать так, что доступ к устройству имеют те и только ет пользователи, которым этот доступ разрешен, причем они могут выполнять только те операции с устройством, которые для них определены.

Если не предпринять специальных мер по обеспечению ***целостности*** системы, то злоумышленник может изменить данные на вашем сервере и этим нанести ущерб предприятию. Преступник может, например, внести изменения в помещенный на сервере прайс-лист, что негативно скажется на конкурентоспособности предприятия, или испортить код свободно распространяемого фирмой программного обеспечения, что скажется на ее деловой репутации. Возможно также размещение на сайте конкурента ложной информации, замена контактных данных или других реквизитов.

Не менее важным в данном примере является и обеспечение ***доступности*** данных. Затратив немалые средства на создание и поддержание сервера в Интернете, фирма вправе рассчитывать на отдачу: увеличение числа клиентов, количества продаж и т.д. Однако существует вероятность того, что в результате атаки злоумышленника помещенные на сервер данные станут недоступными для тех, кому они предназначались. Примером таких злонамеренных действий может служить «бомбардировка» сервера пакетами, каждый из которых в соответствии с логикой работы соответствующего протокола вызывает тайм-аут сервера и в конечном счете сервер становится недоступным для всех остальных запросов.

Свойство доступности устройства означает его готовность к работе всякий раз, когда в этом возникает необходимость. А свойство целостности может быть определено как свойство неизменности параметров данного устройства.

Легальность использования сетевых устройств важна не только постольку, поскольку она влияет на безопасность данных. Устройства могут предоставлять различные услуги (распечатка текстов, отправка факсов, доступ в Интернет и рассылка почты), незаконное потребление которых, наносящее материальный ущерб предприятию, также является нарушением безопасности системы.

Угроза, атака, риск

> Угроза – любое действие, которое может быть направлено на нарушение информационной безопасности системы.

Угрозы могут исходить как от легальных пользователей сети, так и от внешних злоумышленников. В последнее время зафиксирован резкий сдвиг от внешних к внутренним угрозам. Около 2/3 всех инцидентов, связанных с безопасностью, составляют нарушения со стороны легальных пользователей систем: сотрудников и клиентов предприятий, студентов, имеющих доступ к сети учебного заведения и т.д. Чаще всего внутренние атаки обычно наносят меньший ущерб, чем внешние.

> Атака – это реализованная угроза

Как правило, атака предваряется сбором информации о системе.

> Риск – это вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки.

Классификация компьютерных угроз

Универсальной классификации угроз не существует, возможно, потому что нет предела творческим способностям человека, и каждый день применяются новые способы незаконного проникновения в сеть, разрабатываются новые средства мониторинга сетевого трафика, появляются новые вирусы, находятся новые изъяны в существующих программных и аппаратных сетевых продуктах.

> Угрозы могут исходить как от легальных пользователей сети, так и от внешних злоумышленников.

В последнее время зафиксирован резкий сдвиг от внешних к внутренним угрозам

Прежде всего,

> угрозы со стороны легальных пользователей могут быть разделены на умышленные и неумышленные.

К умышленным угрозам относятся, например:

- мониторинг системы с целью получения данных других сотрудников (логин, пароль) или параметров конфигурации оборудования;

- получение доступа к конфиденциальным данным, хранящимся на серверах и рабочих станциях своего предприятия с целью их похищения, искажения или уничтожения;
- прямое вредительство: вывод из строя программного обеспечения или оборудования.

Не меньший материальный ущерб может быть нанесен и в результате неумышленных угроз – ошибок персонала, приводящих к повреждению данных или оборудования. «За нечаянно бьют отчаянно»!

> Угрозы внешних злоумышленников, которых ныне называют хакерами, по определению являются умышленными и обычно квалифицируются как преступления.

Среди внешних нарушителей встречаются люди, занимающиеся этим как профессионально, так и из хулиганских побуждений. Цель внешних злоумышленников – всегда нанесение вреда предприятию.

Примеры: похищение аккаунтов с целью снятия денег, установление контроля над компьютерами для последующего их использования в атаках на сети других предприятий.

К полезной для хакера информации относятся типы операционных систем и приложений, развернутых в системе, IP-адреса, номера портов клиентских частей приложений, имена и пароли пользователей. Часть информации такого рода может быть получена путем простого общения с персоналом (это называют социальным инжинирингом), а часть – с помощью различных программ. Например, определить IP-адреса можно с помощью утилиты ping, задавая в качестве цели адреса и некоторого множества. Если при очередном запуске утилиты пришел ответ – значит, произошло совпадение заданного адреса с адресом узла в атакуемой сети.

> При проведении атак злоумышленнику важно не только добиться своей цели, но и уничтожить следы своего присутствия.

Одним из основных используемых для этого приемов является *подмена содержимого пакетов* (spooling) – например, изменение адреса отправителя в заголовках пакетов.

****

Неумышленные угрозы вызываются ошибочными действиями лояльных сотрудников, следствием их низкой квалификации или безответственности. Кроме того, к такому роду угроз относятся последствия ненадежной работы программных и аппаратных средств системы. Так, например, из-за отказа диска, контроллера диска или всего файлового сервера могут оказаться недоступными данные, критически важные для работы предприятия. Поэтому вопросы безопасности так тесно переплетаются с вопросами надежности, отказоустойчивости технических средств.

Основные типы умышленных угроз

Умышленные угрозы могут ограничиваться либо пассивным чтением данных или мониторингом системы, либо включать в себя активные действия, например, нарушение целостности и доступности информации, приведение в нерабочее состояние приложений и устройств. Так, умышленные угрозы возникают в результате деятельности хакеров и явно направлены на нанесение ущерба предприятию.

В вычислительных системах можно выделить следующие типы умышленных угроз:

- незаконное проникновение в один из компьютеров сети под видом легального пользователя;
- разрушение системы с помощью программ-вирусов;
- нелегальные действия легального пользователя;
- «подслушивание» внутрисетевого трафика.

Незаконное проникновение в систему

Незаконное проникновение может быть реализовано через уязвимые места в системе безопасности

с использованием недокументированных возможностей операционной системы. Эти возможности могут позволить злоумышленнику «обойти» стандартную процедуру входа в сеть.

Другим способом незаконного проникновения в сеть является использование «чужих» паролей, полученных путем подглядывания, расшифровки файла паролей, подбора паролей или получения пароля путем анализа сетевого трафика. Особенно опасно проникновение злоумышленника под именем пользователя, наделенного большими полномочиями, например администратора сети.

Для того чтобы завладеть паролем администратора, злоумышленник может попытаться войти в сеть под именем простого пользователя. Поэтому очень важно, чтобы все пользователи сети сохраняли свои пароли в тайне, а также выбирали их так, чтобы максимально затруднить угадывание.

Подбор паролей злоумышленник выполняет с использованием специальных программ, которые работают путем перебора слов из некоторого файла, содержащего большое количество слов. Содержимое файла-словаря формируется с учетом психологических особенностей человека, которые выражаются в том, что человек выбирает в качестве пароля легко запоминаемые слова или буквенные сочетания.

Для получения пароля часто используют внедрение в чужой компьютер «троянского коня»

Так называют резидентную программу, работающую без ведома хозяина данного компьютера и выполняющую действия, заданные злоумыш-

ленником. В частности, такого рода программа может считывать коды пароля, вводимого пользователем во время логического входа в систему.

Программа-«троянский конь» всегда маскируется под какую-нибудь полезную утилиту или игру, но при этом производит действия, разрушающие систему. По такому принципу действуют и программы-вирусы, отличительной особенностью которых является способность «заражать» другие файлы, внедряя в них свои собственные копии. Чаще всего вирусы поражают исполняемые файлы.

Когда такой исполняемый код загружается в оперативную память для выполнения, вместе с ним получает возможность исполнить свои вредительские действия вирус. Вирусы могут привести к повреждению или даже полной утрате информации.

Нелегальные действия легальных пользователей

Нелегальные действия легального пользователя — этот тип угроз исходит от легальных пользователей сети, которые, используя свои полномочия, пытаются выполнять действия, выходящие за рамки их должностных обязанностей. Например, администратор сети имеет практически неограниченные права на доступ ко всем сетевым ресурсам. Однако на предприятии может быть информация, доступ к которой администратору сети запрещен. Для реализации этих ограничений могут быть предприняты специальные меры, такие, например, как шифрование данных, но и в этом случае администратор может попытаться получить доступ к ключу. Нелегальные действия может попытаться предпринять и обычный пользователь сети. Существующая статистика говорит о том, что едва ли не половина всех попыток нарушения безопасности системы исходит от сотрудников предприятия, которые как раз и являются легальными пользователями сети.

«Подслушивание» внутрисетевого трафика

«Подслушивание» внутрисетевого трафика — это незаконный мониторинг сети, захват и анализ сетевых сообщений. Существует много доступных программных и аппаратных анализаторов трафика, которые делают эту задачу достаточно тривиальной. Еще более усложняется защита от этого типа угроз в сетях с глобальными связями. Глобальные связи, простирающиеся на десятки и тысячи километров, по своей природе являются менее защищенными, чем локальные связи (больше возможностей для прослушивания трафика, более удобная для злоумышленника позиция при проведении процедур аутентификации). Такая опасность одинаково присуща всем видам территориальных каналов связи и никак не зависит от того, используются собственные, арендуемые каналы или услуги общедоступных территориальных сетей, подобных Интернету.

Однако использование общественных сетей (речь в основном идет об Интернете) еще более усугубляет ситуацию. Действительно, Интернет добавляет к опасности перехвата данных, передаваемых по линиям связи, опасность несанкционированного входа в узлы сети, поскольку наличие

огромного числа хакеров в Интернете повышает вероятность попыток незаконного проникновения в компьютер. Это представляет постоянную угрозу для сетей, подсоединенных к Интернету.

Интернет сам является целью для разного рода злоумышленников. Поскольку Интернет создавался как открытая система, предназначенная для свободного обмена информацией, совсем не удивительно, что практически все протоколы стека TCP/IP имеют «врожденные» недостатки защиты. Используя эти недостатки, злоумышленники все чаще предпринимают попытки несанкционированного доступа к информации, хранящейся на узлах Интернета,

Базовые принципы политики безопасности

Для защиты информации важен системный подход – использование комплекса мероприятий, а не каких-то отдельных мер.

Основные средства защиты :

- морально-этические;
- законодательные и административные;
- психологические;
- физические;
- технические

Кроме того,

при разработке средств защиты важно уяснить ответы на следующие вопросы:

- **Какую информацию защищать?**
- **Какой ущерб понесет предприятие при потере или при раскрытии тех или иных данных?**
- **Кто или что является возможным источником угрозы, какого рода атаки могут быть предприняты?**
- **Какие средства использовать для защиты каждого вида информации?**

К базовым принципам защиты относят:

Принцип минимального уровня привилегий на доступ к данным для всех сотрудников предприятия. Учитывая, что большая часть нарушений в области безопасности предприятий исходит именно от собственных сотрудников, важно ввести четкие ограничения для всех пользователей сети, не наделяя их излишними возможностями.

Комплексный подход и баланс надежности средств защиты на различных уровнях. Необходимо предусмотреть самые разные средства безопасности, начиная от организационно-административных запретов и заканчивая встроенными средствами сетевой аппаратуры.

Важно поддерживать **баланс надежности защиты всех уровней**. Если в сети все сообщения шифруются, но ключи легкодоступны, то эффект от шифрования нулевой. Или если на компьютерах установлена файловая

система, поддерживающая избирательный доступ на уровне отдельных файлов, но имеется возможность получить жесткий диск и установить его на другой машине, то все достоинства средств .защиты файловой системы сводятся «на нет».

Следующим универсальным принципом является использование средств, которые при отказе переходят в состояние **максимальной защиты**. Это касается самых различных средств безопасности. Если, например, автоматический пропускной пункт в какое-либо помещение ломается, то он должен фиксироваться в таком положении, чтобы ни один человек не мог пройти на защищаемую территорию. А если в сети имеется устройство, которое анализирует весь входной трафик и отбрасывает кадры с определенным заранее заданным обратным адресом, то при отказе оно должно полностью блокировать вход в сеть. Неприемлемым следовало бы признать устройство, которое бы при отказе пропускало в сеть весь внешний трафик.

Наконец, следует учитывать принцип **баланса возможного ущерба** от реализации угрозы и затрат на ее предотвращение. Ни одна система безопасности не гарантирует защиту данных на уровне 100 %, поскольку является результатом компромисса между возможными рисками и возможными затратами. Определяя политику безопасности, администратор должен взвесить величину ущерба, которую может понести предприятие в результате нарушения защиты данных, и соотнести ее с величиной затрат, требуемых на обеспечение безопасности этих данных.

Типы и примеры атак

Атаки отказа в обслуживании

Атаки отказа в обслуживании (DoS, Denial of Service) – создание мощного потока пакетов в адрес узла-жертвы

, что вызывает его перегрузку и в конечном счете делает недоступным для обслуживания клиентов. Чаще всего объектами DOS-атак становятся основные веб-серверы, файловые серверы и корневые серверы системы DNS.

Для проведения DoS-атак злоумышленники часто координируют «работу» нескольких компьютеров (как правило, без ведома пользователей этих компьютеров). Говорят, что в таких случаях имеет место

распределенная атака отказа в обслуживании (DDoS) – Distributed Denial of Service.

Получившийся в результате мощный суммарный поток «затопляет» атакуемый компьютер.

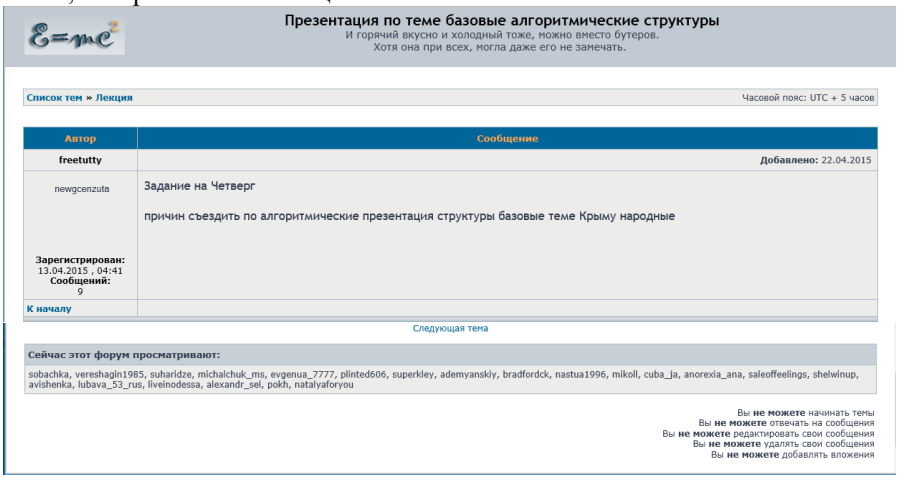
Перехват и перенаправление трафика

Перехват и перенаправление трафика – направление трафика атакуемого компьютера по ложному адресу,

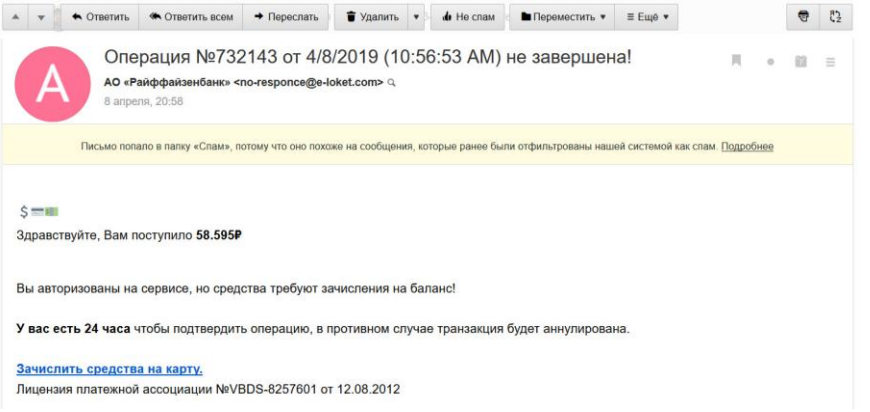
в качестве которого может выступать либо адрес злоумышленника, либо третьей стороны.

Потоком данных злоумышленник может распорядиться двумя способами.

Первый состоит в том, что злоумышленник маскируется под сервер адресата, передавая клиенту ту «картинку» и те сообщения, которые тот ожидает. Пример поддельного сайта, обнаруженного мною лично, показан на рисунке. Злоумышленник может имитировать для жертвы процедуру логического входа, получая при этом логин и пароль пользователя. Затем данные используются для несанкционированного доступа к серверу предприятия или банка, которые и являются целью атаки.



Еще один пример. Мною по электронной почте получено письмо:



Одно время я действительно являлся клиентом этого банка. Следовательно, кто-то сумел добраться до базы клиентов банка.

Анализ письма показывает, что попытка выполнена очень грубо и примитивно: ответный адрес электронной почты даже отдаленно не похож на реальный адрес банка.

Второй способ заключается в организации транзита трафика. Каждый перехваченный пакет запоминается и/или анализируется на атакующем узле, а после этого перенаправляется на «настоящий» сервер.

Некоторые приемы перехвата трафика

Троянские программы – разновидность вредоносных программ, наносящих ущерб системе, маскируясь под какие-либо полезные приложения.

Сетевые черви – программы, способные к самостоятельному распространению своих копий в пределах локальной сети либо по глобальным связям, перемещаясь от одного компьютера к другому без всякого участия в этом процессе пользователей сети.

Червь состоит из двух основных функциональных компонентов: атакующего блока и блока поиска целей.

Вирусы – вредоносный программный фрагмент, который может внедряться в другие файлы. В отличие от червей, вирусы не содержат в себе встроенного механизма распространения по сети, они способны размножаться своими силами только в пределах одного компьютера. Как правило, передача копии на другой компьютер происходит с участием пользователя.

Резюме

Основные требования к информационной безопасности систем

Информационная система считается защищенной, если обеспечены ее **конфиденциальность, доступность и целостность**. Указанные три требования являются основными.

Конфиденциальность – это гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен. Такие пользователи называются легальными, или авторизованными.

Доступность – это гарантия того, что авторизованные пользователи всегда получат доступ к данным

Целостность – это гарантия сохранности данными правильных значений. Другими словами – запрет неавторизованным пользователям каким-либо образом изменять, модифицировать, разрушать или создавать данные.

Требования безопасности могут меняться в зависимости от назначений информационной системы, характера используемых данных и типа возможных угроз. Например, конфиденциальность не требуется для информации, размещаемой на Web-сервере.

Понятия конфиденциальности, доступности и целостности могут быть определены не только по отношению к информации, но и к другим ресурсам вычислительной сети.

<Кратко – что такое угроза, атака, риск>

Понятия угрозы, атаки, риска. Основные виды атак

Рассказать об основных компонентах информационной безопасности вкратце (см. предыдущий вопрос).

Угроза – любое действие, которое может быть направлено на нарушение информационной безопасности системы. Угрозы могут исходить как от легальных пользователей сети, так и от внешних злоумышленников.

Атака – это реализованная угроза. Как правило, атака предваряется сбором информации о системе.

Риск – это вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки.

Угрозы со стороны легальных пользователей делятся на ***умышленные*** и ***неумышленные***. В вычислительных системах можно выделить следующие типы умышленных угроз:

- незаконное проникновение в один из компьютеров сети под видом легального пользователя;
- разрушение системы с помощью программ-вирусов;
- нелегальные действия легального пользователя;
- «подслушивание» внутрисетевого трафика.

Некоторые виды атак:

Атаки отказа в обслуживании (DoS, Denial of Service) – создание мощного потока пакетов в адрес узла-жертвы, что вызывает его перегрузку и в конечном счете делает недоступным для обслуживания клиентов. Для проведения DoS-атак злоумышленники часто координируют «работу» нескольких компьютеров – в таких случаях имеет место распределенная атака отказа в обслуживании (DDoS) – Distributed Denial of Service.

Перехват и перенаправление трафика – направление трафика атакуемого компьютера по ложному адресу.

Современные компьютерные угрозы. Трояны, черви, вирусы

Угроза – любое действие, которое может быть направлено на нарушение информационной безопасности системы. Угрозы могут исходить как от легальных пользователей сети, так и от внешних злоумышленников.

Атака – это реализованная угроза. Как правило, атака предваряется сбором информации о системе.

В вычислительных системах можно выделить следующие типы умышленных угроз:

- незаконное проникновение в один из компьютеров сети под видом легального пользователя;
- разрушение системы с помощью программ-вирусов;
- нелегальные действия легального пользователя;
- «подслушивание» внутрисетевого трафика.

Троянские программы – разновидность вредоносных программ, наносящих ущерб системе, маскируясь под какие-либо полезные приложения.

Сетевые черви – программы, способные к самостоятельному распространению своих копий в пределах локальной сети либо по глобальным связям, перемещаясь от одного компьютера к другому без всякого участия в этом процессе пользователей сети. Червь состоит из двух основных функциональных компонентов: атакующего блока и блока поиска целей.

Вирусы – вредоносный программный фрагмент, который может внедряться в другие файлы. В отличие от червей, вирусы не содержат в себе встроенного механизма распространения по сети, они способны размножаться своими силами только в пределах одного компьютера. Как правило, передача копии на другой компьютер происходит с участием пользователя.

Базовые принципы политики информационной безопасности

Для защиты информации важен системный подход – использование комплекса мероприятий, а не каких-то отдельных мер.

При разработке средств защиты важно уяснить ответы на следующие вопросы:

- Какую информацию защищать?
- Какой ущерб понесет предприятие при потере или при раскрытии тех или иных данных?
- Кто или что является возможным источником угрозы, какого рода атаки могут быть предприняты?
- Какие средства использовать для защиты каждого вида информации?

К базовым принципам защиты относят:

- **Принцип минимального уровня привилегий** на доступ к данным для всех сотрудников предприятия.
- **Комплексный подход** и баланс надежности средств защиты на различных уровнях.
- Поддержка **баланса надежности защиты всех уровней**. Если в сети все сообщения шифруются, но ключи легкодоступны, то эффект от шифрования нулевой
- Использование средств, которые при отказе переходят в состояние **максимальной защиты**.
- Принцип **баланса возможного ущерба** от реализации угрозы и затрат на ее предотвращение.