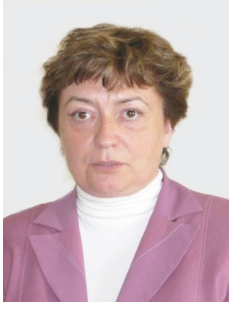

Лапонина Ольга Робертовна
Преподаватель магистратуры факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова.

Защита информации в сети Интернет: основные термины и технологии

Сегодня подключение корпоративной сети к Интернету стало обыденным явлением. Большинство современных компаний имеют собственные сайты в Интернете. За удобства и новые возможности приходится расплачиваться появлением новых проблем, связанных с безопасностью. И в первом, и во втором случаях для того, чтобы не иметь сложностей, связанных с нежелательным присутствием посторонних в вашей корпоративной сети или на сайте, необходимо учитывать многие аспекты и достаточно свободно разбираться во многих технологиях. Для обеспечения безопасности приходится создавать так называемую «оборону вглубь», потому что не существует единственного универсального средства или единственной универсальной технологии, которые позволили бы решить все проблемы информационной безопасности.

За несколько последних десятилетий требования к защите информации существенно изменились. До начала широкого использования автоматизированных систем обработки данных защита информации достигалась исключительно надёжными замками, охраной помещений и административными мерами. С появлением компьютеров стала очевидной необходимость использования автоматических средств защиты файлов данных и программной среды. Следующий этап развития автоматических средств защиты связан с появлением распределённых систем обработки данных и компьютерных сетей, в которых средства сетевой безопасности используются в первую очередь для защиты передаваемых по сетям данных.

Вопросы защиты информации несомненно являются одними из самых важных при развёртывании сетей и подключении их к Интернету.

Какие же проблемы, связанные с безопасностью, возникают при использовании компьютерных сетей?

1. Фирма имеет несколько офисов, расположенных на достаточно

большом расстоянии друг от друга. При пересылке конфиденциальной информации по общедоступной сети (например, Интернет) необходимо быть уверенным, что никто не сможет ни подсмотреть, ни изменить эту информацию.

2. Сетевой администратор осуществляет удалённое управление компьютером. Кто-то другой перехватывает это управляющее сообщение, изменяет его содержание и отправляет сообщение на данный компьютер.

3. Пользователь несанкционированно получает доступ к удалённому компьютеру с правами законного пользователя, либо, имея право доступа к компьютеру, получает доступ с гораздо большими правами.

4. Фирма открывает интернет-магазин, который принимает оплату в электронном виде. В этом случае продавец должен быть уверен, что он отпускает товар, который действительно оплачен, а покупатель должен иметь гарантии, что он, во-первых, получит оплаченный товар, а во-вторых, номер его кредитной карточки не станет никому известен.

5. Фирма открывает свой сайт в Интернете. В какой-то момент содержимое сайта заменяется новым либо возникает такой поток и такой способ обращений к сайту, что сервер не справляется с обработкой запросов. В результате обычные посетители сайта либо видят информацию, не имеющую к фирме никакого отношения, либо просто не могут попасть на сайт фирмы.

В нашей статье средствами сетевой безопасности мы будем называть меры **предотвращения нарушений безопасности**, которые возникают при передаче информации по сетям, а также меры, позволяющие **определять, что такие нарушения безопасности имели место**.

Рассмотрим основные понятия, относящиеся к защите информации, и их взаимосвязи.

Любая информация должна кому-то принадлежать, кто будет заботиться о её защите. Эта информация должна быть для него важной и ценной, иначе не стоит её защищать. Поэтому мы говорим не просто об информации, а об информационных ценностях. Кроме того, эта информация должна представлять определённый интерес ещё для кого-то, кто будет пытаться получить к ней доступ, но кому собственник информации не хочет давать эту информацию. Этого человека (или программу, запущенную этим человеком) будем называть нарушителем, атакующим или оппонентом.

Собственник определяет множество **информационных ценностей**, которые должны быть защищены от различного рода **атак**. Атаки осуществляются **противниками** или **оппонентами**, использующими различные **уязвимости** в защищаемых ценностях. Основными нарушениями безопасности являются раскрытие информационных ценностей (потеря конфиденциальности), их несанкционированная (неавторизованная) модификация (потеря целостности) или неавторизованная потеря доступа к этим ценностям (потеря доступности).

Собственники информационных ценностей анализируют уязвимости защищаемых ресурсов и возможные

атаки, которые могут иметь место в данных условиях. В результате такого анализа определяются **риски** для данного набора информационных ценностей. Этот анализ определяет выбор контрмер, которые задаются **политикой безопасности** и обеспечиваются с помощью **механизмов и сервисов безопасности**. Следует учитывать, что отдельные уязвимости могут сохраниться и после применения механизмов и сервисов безопасности.

На рис. 1 показана взаимосвязь рассмотренных выше понятий информационной безопасности.

Рис. 1. Взаимосвязь основных понятий безопасности информационных систем

Поясним некоторые термины, которые были введены выше.

Уязвимость – слабое место в системе, с использованием которого может быть осуществлена атака.

Риск – вероятность того, что конкретная атака будет осуществлена с использованием конкретной уязвимости. В конечном счёте, каждая организация должна принять решение о допустимом для неё уровне риска. Это решение должно найти отражение в политике безопасности, принятой в организации.

Политика безопасности – правила, директивы и практические навыки, которые определяют то, как информационные ценности обрабатываются, защищаются и распространяются в организации и между информационными системами; набор критериев для предоставления сервисов безопасности.

Атака – любое действие, нарушающее безопасность информационной системы. Атакой может быть не только отдельное действие, но и последовательность связанных между собой действий, использующих *уязвимости* данной информационной системы и приводящих к нарушению *политики безопасности.*

Механизм безопасности – программное или аппаратное средство, которое определяет или предотвращает атаку.

Сервис безопасности – сервис, который обеспечивает задаваемую политикой безопасности защиту систем и передаваемых данных либо констатирует осуществление атаки. Сервис использует один или более механизмов безопасности.

Далее мы остановимся более подробно на некоторых наиболее важных понятиях.

Защита информации в сетях

Виды сетевых атак

Взаимодействие по сети означает, что существует информационный поток данных от отправителя к получателю. Отправителем и получателем в данном случае могут являться как компьютеры, так и отдельные программы, запущенные на этих компьютерах.

Рис. 2. Информационный поток

Все атаки на информационную систему можно разделить на пассивные и активные.

1. Пассивная атака. Пассивной называется такая атака, при которой противник не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения. Целью пассивной атаки может быть только **прослушивание передаваемых сообщений и анализ трафика**.

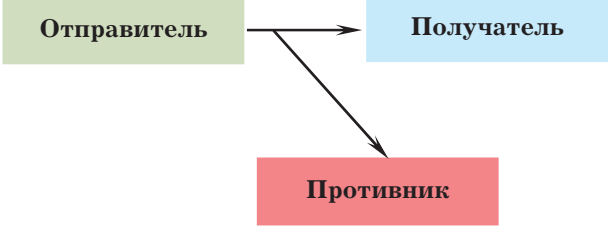

Рис. 3. Пассивная атака

2. Активная атака. Активной называется такая атака, при которой противник имеет возможность **модифицировать передаваемые сообще-**

ния и вставлять свои сообщения. Различают следующие типы активных атак.

- **Отказ в обслуживании – DoS-атака (Denial of Service)**

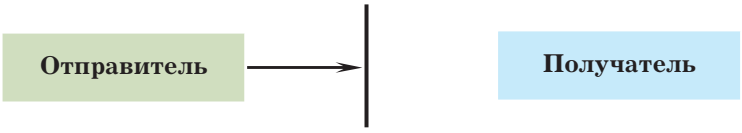

Рис. 4. DoS-атака

Отказ в обслуживании нарушает нормальное функционирование сетевого сервиса (в данном случае Получателя), когда законный пользователь (в данном случае Отправитель) не может получить сетевой сервис.

- **Модификация потока данных – атака «man in the middle»**

Модификация потока данных означает либо изменение содержимого пересылаемого сообщения, либо изменение порядка сообщений.

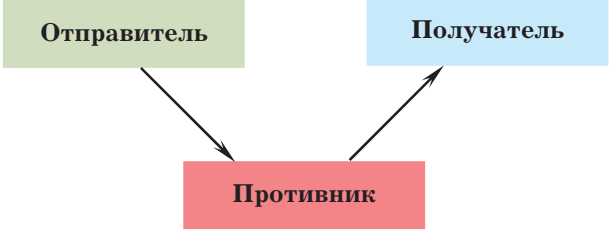

Рис. 5. Атака «man in the middle»

- **Создание ложного потока (фальсификация)**

Фальсификация (нарушение аутентичности) означает попытку одного субъекта выдать себя за другого. В данном случае Отправитель не передаёт никакого сообщения, а Противник пытается выдать себя за Отправителя.

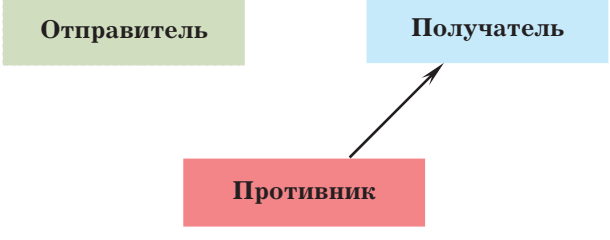

Рис. 6. Создание ложного потока

- **Повторное использование**

Повторное использование означает перехват данных с последующей их пересылкой через некоторое время Получателю для получения несанкционированного доступа – это так называемая replay-атака. На самом деле replay-атаки являются одним из вариантов фальсификации, но в силу того, что это один из наиболее распространённых вариантов атаки для получения несанкционированного доступа, его часто рассматривают как отдельный тип атаки.

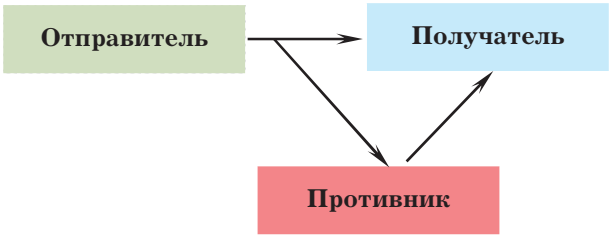

Рис. 7. Replay-атака

Перечисленные атаки могут существовать в любых типах сетей, а не только в сети Интернет. Но в сети Интернет эти атаки встречаются чаще, потому что, во-первых, Интернет стал самой распространённой сетью, а во-вторых, при разработке протоколов, которые используются в сети Интернет, требования безопасности никак не учитывались.

Основные сервисы безопасности

Конфиденциальность – предотвращение пассивных атак для передаваемых или хранимых данных. Сервис конфиденциальности преобразует передаваемое сообщение таким образом, чтобы никто, кроме Получателя, не мог понять передаваемое сообщение. Для всех остальных передаваемое сообщение должно казаться случайным набором нулей и единиц.

Аутентификация – подтверждение того, что информация получена от законного Отправителя и Получатель действительно является тем, за кого себя выдаёт. В случае передачи единственного сообщения аутентификация должна гарантировать, что получателем сообщения является тот, кто нужно, и сообщение получено из заявленного источника. В случае, когда между Отправителем и Получателем передаётся поток сообщений в обе стороны, необходимо решить две задачи. Во-первых, при инициализации соединения сервис должен гарантировать, что оба участника являются законными. Во-вторых, сервис должен гарантировать, что на соединение никто не воздействует таким образом, что третья сторона сможет маскироваться под одну из легальных сторон уже после установления соединения.

Целостность – сервис, гарантирующий, что информация при хранении или передаче не изменилась. Сервис может иметь дело с потоком сообщений, единственным сообщением или отдельными полями в сообщении, а также с хранимыми файлами и отдельными записями файлов.

Невозможность отказа – невозможность как для Получателя, так и для Отправителя, отказаться от факта передачи. Таким образом, когда сообщение отправлено, Получатель может убедиться, что это сделал легальный Отправитель. Аналогично, когда сообщение пришло, Отправитель может убедиться, что оно получено легальным Получателем.

Контроль доступа – возможность ограничить и контролировать доступ к компьютерам и программам по коммуникационным линиям.

Доступность – результатом атак может быть потеря или снижение доступности того или иного сервиса. Данный сервис предназначен для того, чтобы минимизировать возможность осуществления DoS-атак.

Механизмы безопасности

Для предотвращения атаки могут применяться как программные, так и аппаратные средства. В частности, различные алгоритмы шифрования передаваемой информации.

Алгоритмы симметричного шифрования – криптографические алгоритмы, предназначенные для преобразования сообщения таким образом, чтобы невозможно было получить исходное сообщение без знания некоторой дополнительной информации, называемой **ключом**. Такое преобразование называется **шифрованием**. Обратное преобразование зашифрованного сообщения в исходное называется **расшифрованием**. В этих алгоритмах для шифрования и расшифрования используется один и тот же ключ, поэтому эти алгоритмы называется **симметричными**.

Алгоритмы асимметричного шифрования – криптографические алгоритмы, в которых для шифрования и расшифрования используются **два разных ключа**, называемые **открытым и закрытым ключами**, причём, **зная закрытый ключ, вычислить открытый невозможно**.

Хэш-функции – криптографические функции, входным значением которых является сообщение произвольной длины, а выходным значением – сообщение фиксированной длины. Хэш-функции обладают рядом свойств, которые позволяют с высокой долей вероятности определять изменение входного сообщения.

Защита информации при сетевом взаимодействии

Безопасное сетевое взаимодействие в общем виде можно представить следующим образом (рис. 8).

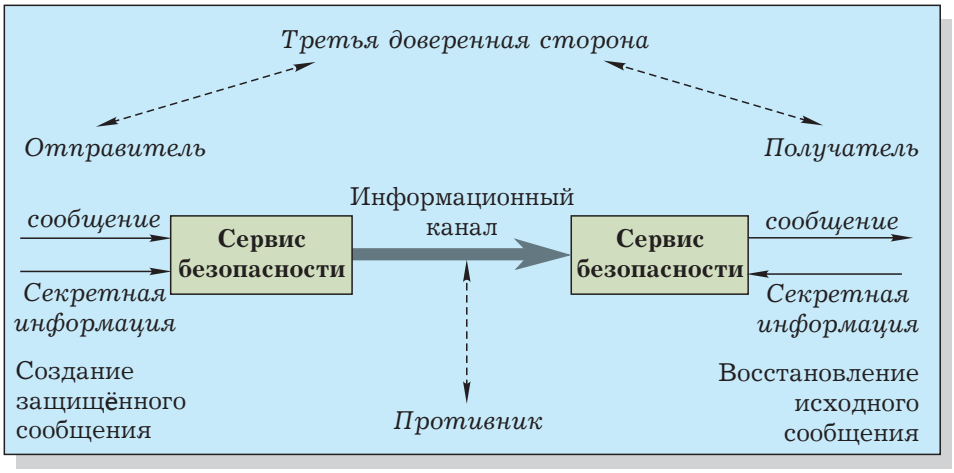

Рис. 8. Защита информации при сетевом взаимодействии

Сообщение, которое передаётся от одного участника другому, проходит через множество других компьютеров с использованием большого количества протоколов. Можно считать, что устанавливается информационный канал от Отправителя к Получателю. Сервисы безопасности должны обеспечивать защиту этого информационного канала от всех типов атак, о которых мы уже говорили.

Средства защиты необходимы, если требуется защитить передаваемую информацию от противника, который может представлять угрозу конфиденциальности, аутентификации, целостности и т. п.

Говоря о технологиях повышения безопасности, имеют в виду два момента.

1. Передача информации производится в зашифрованном виде. Сообщение изменяется таким образом, что противнику кажется случайным набором нулей и единиц. Возможно, в сообщение добавляются данные для обеспечения целостности сообщения, т. е. данные, которые позволяют Получателю с большой долей вероятности определить, что сообщение не было изменено.

2. Обоим участникам обмена данных должна быть известна некоторая секретная информация, которая не известна противнику. Эта информация используется для шифрования сообщения.

Кроме того, в некоторых случаях для обеспечения безопасной передачи бывает необходима Третья Доверенная Сторона (Third Trusted Party – TTP). Например, третья сторона может быть ответственной за распределение между двумя участниками секретной информации, которая не стала бы доступна противнику. Либо третья сторона может использоваться для решения споров между двумя участниками относительно достоверности передаваемого сообщения.

Из данной общей модели вытекают следующие три основные задачи, которые необходимо решить при разработке конкретного сервиса безопасности.

1. Разработка алгоритма шифрования/расшифрования для выполнения безопасной передачи информации. Алгоритм должен быть таким, чтобы противник не мог расшифровать перехваченное сообщение, не зная секретную информацию.

2. Создание секретной информации с использованием алгоритма шифрования.

3. Разработка протокола обмена сообщениями для распределения разделяемой секретной информации таким образом, чтобы она не стала известна противнику.

Защита информационной системы

Другой ситуацией, относящейся к защите информации, является обеспечение безопасности некоторой информационной системы, к которой необходимо предотвратить нежелательный доступ. Общую схему этих ситуаций можно проиллюстрировать следующим образом (рис. 9).

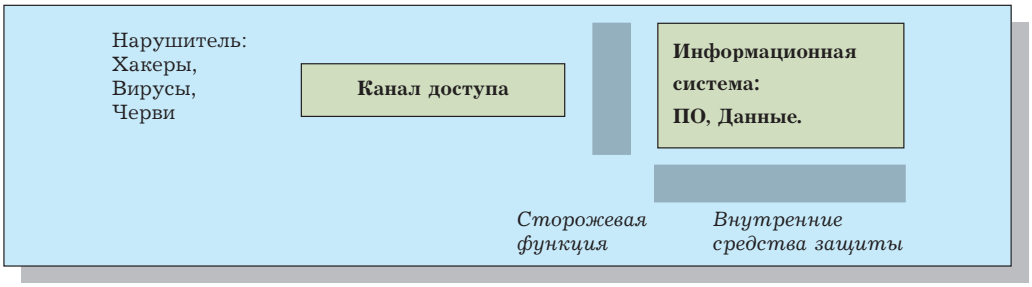

Рис. 9. Модель безопасности информационной системы

Хакер, который пытается осуществить незаконное проникновение в системы, доступные по сети, может просто получать удовольствие от взлома, а может стараться повредить информационную систему и/или внедрить в неё что-нибудь для своих целей. Например, целью хакера может быть получение номеров кредитных карточек, хранящихся в системе.

Другим типом нежелательного доступа является размещение в вычислительной системе чего-либо, что каким-то образом изменяет работу программ в компьютере. Таким образом, существует два типа атак.

1. Доступ к информации с целью получения или модификации хранящихся в системе данных.

2. Атака на сервисы, чтобы помешать использовать их или нарушить их работу.

Вирусы и черви – примеры подобных атак.

Сервисы безопасности, которые предотвращают нежелательный доступ, можно разбить на две категории.

1. Первая категория определяется в терминах **сторожевой** функции. Эти механизмы включают процедуры входа, основанные, например, на использовании пароля, что позволяет разрешить доступ только авторизованным пользователям. Также они включают различные межсетевые экраны (firewalls), которые предотвращают атаки и, в частности, позволяют предупреждать проникновение червей, вирусов и т. п.

2. Вторая линия обороны состоит из различных внутренних мониторов, контролирующих доступ и анализирующих деятельность пользователей.

Одним из основных понятий при обеспечении безопасности информационной системы является понятие *авторизации* – определение и предоставление прав доступа к конкретным ресурсам или программам.

Юмор Юмор Юмор Юмор Юмор Юмор

– Как мне восстановить разбитую на две части чашку без клея?
– Плотно прижать эти части друг к другу и никогда не отпускать.