УДК 004.056.5

С.В. Матвеев

Меры защиты от скрытых каналов в автоматизированных системах и их пропускная способность при некоторых способах противодействия

Оценка защищенности информации в компьютерных сетях в значительной степени зависит от потенциальных возможностей нарушителя, которые могут использоваться для компрометации информации, в том числе с применением скрытых каналов. Для случая соединения двух сегментов сети посредством граничного маршрутизатора приведена классификация возможностей построения скрытых каналов нарушителем. Рассмотрены меры, обеспечивающие защиту от построения скрытых каналов. Для нескольких методов защиты от скрытых каналов, манипулирующих скоростью передачи данных в канале, приведены оценки пропускной способности.

Ключевые слова: автоматизированная система, скрытые каналы, пропускная способность.

Скрытые каналы в автоматизированных системах

Построение защищенных автоматизированных систем (АС) в настоящее время не может обойтись без оценки угроз безопасности, связанных со скрытыми информационными каналами. Скрытым каналом (СК) является коммуникационный канал, не предусмотренный разработчиком, использующийся для нарушения политики безопасности системы [1].

Наличие или возможность построения скрытых каналов в автоматизированной системе может повлечь за собой как утечку конфиденциальной информации из АС, так и негативное, возможно, деструктивное влияние извне на деятельность АС.

Рассмотрим возможности по построению скрытых каналов и меры по противодействию им для автоматизированной системы представляющей собой несколько распределенных сегментов корпоративных сетей, объединенных между собой коммуникационными каналами.

Рассмотрим схему взаимодействия скрытого канала с автоматизированной системой и средствами защиты (рис. 1),

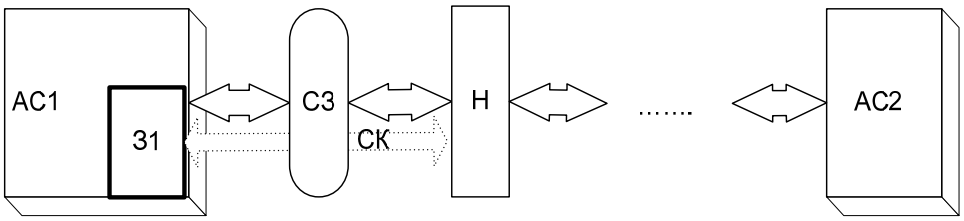

Рис. 1. Схема взаимодействия скрытого канала и автоматизированной системы

где АС1, АС2 – два сегмента автоматизированной системы, соединенных через сеть общего пользования через средства защиты (СЗ); СЗ – средства защиты АС; Н – внешний нарушитель, осуществляющий несанкционированный доступ к АС либо оказывающий негативное влияние на неё; З1 – внутренний нарушитель системы, формирующий скрытый канал для связи с внешним нарушителем Н.

В настоящее время принято выделять скрытые каналы по памяти, скрытые каналы по времени и скрытые статистические каналы. Для построения подобных скрытых каналов в IP-сетях применяются:

К1 – внедрение данных в неиспользуемые поля передаваемых или принимаемых объектов (пакетов);

К2 – внедрение данных в информационные объекты, приводящее к внешне невидимым изменениям данных объектов;

К3 – изменение длин передаваемых пакетов;

К4 – изменение длин межпакетных интервалов;

К5 – манипуляция адресами отправителя или получателя.

Для того чтобы иметь возможность построить скрытый канал, нарушитель, внутренний и внешний, должен обладать следующими возможностями:

В1 – иметь возможность изменять содержимое служебных полей любого истинного передаваемого пакета (для построения каналов типа К1);

В2 – иметь возможность изменять информационное содержимое любого истинного передаваемого пакета (для построения каналов типа К2);

В3 – может изменять длину любого пакета (для построения каналов типа К3);

В4 – может формировать собственные ложные IP-пакеты произвольной длины (для построения каналов типа К3, К4, К5);

В5 – может буферизовать все пакеты, подлежащие передаче из внутренней или внешней сети, и передавать в канал в заранее определенный момент времени (для построения каналов типа К3, К4, К5);

В6 – иметь полную информацию о топологии используемой сети связи (для построения каналов типа К5).

Меры по ограничению возможностей внутреннего нарушителя по доступу к конфиденциальной информации или к критичным ресурсам в автоматизированной системе в настоящей работе не рассматриваются. Предполагается, что внутренний нарушитель имеет полный или частичный доступ к защищаемой информации или защищаемому ресурсу.

Для обеспечения защиты автоматизированных систем от организации скрытых каналов в средствах защиты в настоящее время применяются следующие механизмы защиты:

З1 – нормализация неиспользуемых полей пакетов трафика;

З2 – нормализация длин пакетов;

З3 – нормализация длин межпакетных интервалов;

З4 – нормализация процесса передачи пакетов различным адресатам;

З5 – контроль и фильтрация пакетов по заданным правилам (межсетевое экранирование);

З6 – переформирование пакетов, передаваемых или принимаемых из коммуникационной среды (использование прокси-серверов);

З7 – туннелирование трафика с использованием алгоритмов криптографической защиты, таких как шифрование и имитозащита.

Ниже (табл. 1) приведено соответствие между возможностями нарушителя и алгоритмами, реализованными в средствах защиты, обеспечивающих защиту от построения скрытых каналов в автоматизированных системах от угроз У1 и У2. Заметим, что для защиты от угрозы утечки конфиденциальной информации (У1) описываемая мера защиты должна применяться для исходящего трафика, для защиты от угрозы негативного влияния на АС извне (У2) соответствующая мера защиты должна применяться к входящему трафику.

Таблица 1

Взаимосвязь между возможностями нарушителя и мерами защиты

	З1	З2	З3	З4	З5	З6	З7
В1	+	–	–	–	$\pm^{*1}$	$+^{*1}$	+
В2	–	–	–	–	–	$\pm$	+
В3	–	+	–	–	$\pm^{*1}$	$+^{*1}$	–
В4	–	–	$\pm$	–	$\pm^{*1}$	–	+
В5	–	–	+	–	–	–	–
В6	–	–	–	+	–	–	–

В таблице «+» – обозначает полную защиту от построения скрытых каналов в случае наличия у противника данной возможности; «±» – обозначает частичную защиту или защиту при определенных ограничениях на возможности нарушителя; «–» – защита не обеспечивается. «^{*1}» – защита может быть обеспечена при правильном задании правил.

Нетрудно видеть, что полную защиту от организации скрытых каналов в данном случае можно обеспечить, применяя средство защиты, обеспечивающее туннелирование трафика с использованием алгоритмов шифрования и имитозащиты, выравнивание длин пакетов, длин межпакетных интервалов и обеспечивающее равномерную передачу пакетов всем возможным обособленным сегментам автоматизированной системы. К сожалению, алгоритмы, обеспечивающие гарантированное выравнивание длин межпакетных интервалов и равномерную передачу данных всем абонентам сети, негативно сказываются на общей пропускной способности коммуникационных каналов. На практике

указанную совокупность мер защиты можно применять только для случая соединения двух сегментов сети по схеме точка–точка с использованием выделенных линий связи. При этом основное негативное влияние на работоспособность сети связи, оказывает мера защиты, обеспечивающая постоянную длину межпакетного интервала, т.е., по сути, установление постоянной скорости передачи информации.

Таким образом, для критически важных объектов необходимо использовать меры защиты, обеспечивающие полную защиту от организации скрытых каналов. В остальных случаях необходимо реализовывать совокупность мер защиты, обеспечивающих снижение пропускной способности возможных скрытых каналов до уровня, не представляющего серьёзной угрозы безопасности автоматизированной системы. Вопрос определения допустимого уровня пропускной способности скрытого канала конкретной АС является отдельной сложной задачей и в настоящее время полностью не решен.

Алгоритмы нормализации длин межпакетных интервалов и оценка пропускной способности скрытых каналов

Как указано ранее, наибольшее негативное влияние на коммутационный канал оказывает мера защиты, реализующая выравнивание (нормализацию) длин межпакетных интервалов для передаваемых IP-пакетов.

Рассмотрим следующие меры снижения пропускной способности скрытого канала, манипулирующего изменением длин межпакетных интервалов.

1. Передача данных осуществляется пакетами фиксированной длины.

2. В течение определенного интервала передача данных осуществляется с постоянной скоростью.

3. Задается минимальный ограничительный интервал T, определяющий количество переданной через средство защиты информации, через которое возможно как уменьшение, так и увеличение, скорости передачи.

4. Изменение скорости производится на заранее определенную фиксированную величину.

Возможна следующая модификация данного метода:

4.1. Изменение скорости передачи возможно только в моменты $T \cdot k$.

Рассмотрим следующие способы построения скрытых каналов в случае использования этих мер защиты. Предполагаем, что внутренний нарушитель для построения скрытых каналов имеет возможности В1–В6.

Способ 1. Пусть имеется двоичный канал, по которому передаются единичные последовательности длительности T. Рассмотрим наиболее простой способ кодирования информации в этом случае. Нарушитель кодирует информацию следующим способом:

$$\begin{cases} \text{скорость изменилась} \to 0, \\ \text{скорость не изменилась} \to 1. \end{cases}$$

Предполагая, что кодируемые значения 0 и 1 равновероятны, получаем следующую оценку пропускной способности скрытого канала: $C = 1/T$.

Способ 2. Пусть имеется двоичный канал, по которому передаются единичные последовательности длительности T. В случае реализации меры защиты 3 нарушитель кодирует информацию следующим способом: {в момент времени $T + k$ скорость изменилась $\to k$}, где $k \in [0, .., M - 1]$.

Предполагая, что величина k равномерно распределена в интервале $[0, M - 1]$, получаем следующую оценку пропускной способности скрытого канала:

$$C = \frac{1}{\ln(2)} \frac{W\left(\frac{2T-1}{e}\right)}{T - \frac{1}{2}}, \tag{1}$$

где $W(x)$ – функция Ламберта, определяемая как корень уравнения $y \cdot \exp(y) = x$. При значениях $T \to \infty$ пропускная способность

$$C \to \frac{\log_2(2T) - \log_2(e \cdot \ln(2T))}{T}\left(1 - \frac{1}{\ln(2T)}\right). \tag{2}$$

Способ 2.1. Пусть имеется двоичный канал, по которому передаются единичные последовательности длительности T. В случае реализации меры защиты 4.1 нарушитель кодирует информацию следующим способом: {в момент времени $T \cdot k$ скорость изменилась $\rightarrow k$}, где $k \in [0, ..., M-1]$.

Предполагая, что величина k равномерно распределена в интервале [0, M – 1], получим следующую оценку максимальной пропускной способности скрытого канала: $C = \frac{e}{T}$.

Таблица 2

Пропускная способность СК

T	10	100	1000	10000	100000
Способ 1	0,1	10^{-2}	10^{-3}	10^{-4}	10^{-5}
Способ 2	0,23	$4{,}5 \cdot 10^{-2}$	$7{,}2 \cdot 10^{-3}$	10^{-3}	$1{,}3 \cdot 10^{-4}$
Способ 2.1	0,54	$5{,}4 \cdot 10^{-2}$	$5{,}4 \cdot 10^{-3}$	$5{,}4 \cdot 10^{-4}$	$5{,}4 \cdot 10^{-5}$

Заметим, что пропускная способность скрытого канала оценивалась при условии отсутствия шумов в канале.

Приведем (табл. 2) оценки пропускной способности СК для указанных способов противодействия для различных значений T.

Таким образом, можно сделать следующие выводы:

Полную защиту от организации скрытых каналов в данном случае можно обеспечить, применяя средство защиты, обеспечивающее туннелирование трафика с использованием алгоритмов шифрования и имитозащиты, выравнивание длин пакетов, длин межпакетных интервалов и обеспечивающее равномерную передачу пакетов всем возможным обособленным сегментам автоматизированной системы.

При частичной нормализации скорости исходящего трафика существует возможность построения скрытого канала в автоматизированной системе.

Наименьшую скорость передачи информации по скрытому каналу, из описанных выше, обеспечивает возможность изменения скорости передачи информации в моменты времени кратные заранее заданной величине T. Для предложенного способа защиты величина T является критерием защищенности системы.

Литература

1. ГОСТ Р 53113.1–2008 Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. – Ч. 1: Общие положения. – М.: Стандартинформ, 2009. – 7 с.

2. ГОСТ Р 53113.2–2009 Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. – Ч. 2: Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов. – М.: Стандартинформ, 2009. – 8 с.

Матвеев Сергей Васильевич
Зам. нач. отдела Пензенского филиала ФГУП «НТЦ «Атлас»
Тел.: 8-(8412) 20-71-95
Эл. почта: matemat@rambler.ru

Matveev S.V.

Methods of protection from the covert channels in the automated systems and their channel capacity at some modes of opposition.

The estimation of security of the information in computer networks substantially depends on potential possibilities of the infringer which can be used for unauthorized access to information, including with application to covert channels. Classification of possibilities of construction of the covert channels by the infringer for a case of connection of two segments of a network by means of a boundary router is resulted. Methods providing protection against construction of the covert channels are considered. Estimations of throughput for several methods of protection against the covert channels manipulating in the speed of data transmission in the channel are resulted.

Keywords: automated system, covert channel, throughput.