Анна И. Белозубова[1], Константин Г. Когос[2], Филипп В. Лебедев[3]
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: AIBelozubova@mephi.ru, https://orcid.org/0000-0002-1223-5443
[2]e-mail: KGKogos@mephi.ru, https://orcid.org/0000-0002-8090-678X
[3]e-mail: FVLebedev@mephi.ru, https://orcid.org/0000-0002-7120-0750

ОГРАНИЧЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ СЕТЕВЫХ СКРЫТЫХ КАНАЛОВ ПО ВРЕМЕНИ ПУТЕМ ВВЕДЕНИЯ ДОПОЛНИТЕЛЬНЫХ СЛУЧАЙНЫХ ЗАДЕРЖЕК ПЕРЕД ОТПРАВКОЙ ПАКЕТА*

DOI: http://dx.doi.org/10.26583/bit.2021.4.06

Аннотация. Внимание к скрытым каналам во многом увеличилось благодаря опубликованным Э. Сноуденом документам, в которых описывались программные и аппаратные закладки, реализующие недекларированные возможности скрытой передачи информации в сетевом оборудовании компаний Huawei и Juniper, мобильных телефонах компании Apple, компьютерах с операционной системой Windows XP. Скрытый канал может быть построен с использованием любых информационных технологий, однако зачастую злоумышленники строят скрытые каналы в IP-сетях, так как они широко распространены, имеют высокую скорость передачи информации, а повсеместные меры обеспечения безопасности информации, такие как шифрование трафика, не влияют на возможность скрытой передачи информации по некоторым типам таких каналов. Перспективным направлением противодействия утечке информации по сетевым скрытым каналам признано ограничение их пропускной способности. В статье рассматриваются сетевые скрытые каналы по времени, приводится способ оценки их пропускной способности, предлагают и исследуют способ противодействия утечке информации по таким скрытым каналам с помощью введения шума путем введения задержек перед отправкой пакетов, значения которых распределены двумя различными способами: равномерно и, согласно распределению, с убывающей функцией плотности вероятности. В качестве эксперимента были получены временные характеристики IP-трафика от хоста во внутренней сети до общедоступного сервиса, которые использовались для верификации полученных способов оценки пропускной способности скрытых каналов. Отличительной особенностью проводимых расчетов является иллюстрация возможности минимизации нагрузки на канал связи при введении метода противодействия, а также принятие в расчет того факта, что возможность нарушителя наблюдать за текущими условиями в сети позволяет ему подстраивать параметры передачи информации под нагрузку в коммуникационном канале, тем самым поддерживая максимально возможную пропускную способность скрытого канала.

Ключевые слова: скрытые каналы, утечка информации, задержки, пропускная способность, ограничение.

Для цитирования: БЕЛОЗУБОВА, Анна И.; КОГОС, Константин Г.; ЛЕБЕДЕВ, Филипп В. ОГРАНИЧЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ СЕТЕВЫХ СКРЫТЫХ КАНАЛОВ ПО ВРЕМЕНИ ПУТЕМ ВВЕДЕНИЯ ДОПОЛНИТЕЛЬНЫХ СЛУЧАЙНЫХ ЗАДЕРЖЕК ПЕРЕД ОТПРАВКОЙ ПАКЕТА. Безопасность информационных технологий, [S.l.], т. 28, № 4, с. 74–89, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1378. DOI: http://dx.doi.org/10.26583/bit.2021.4.06.

Благодарности. Исследование выполнено при поддержке Министерства науки и высшего образования Российской Федерации (грант для молодых ученых на исследования в области информационной безопасности в цифровой экономике).

Anna I. Belozubova[1], Konstantin G. Kogos[2], Philipp V. Lebedev[3]
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
[1]e-mail: AIBelozubova@mephi.ru, https://orcid.org/0000-0002-1223-5443/
[2]e-mail: KGKogos@mephi.ru, https://orcid.org/0000-0002-8090-678X

[3]*e-mail: FVLebedev@mephi.ru, https://orcid.org/0000-0002-7120-0750*

Network covert channels capacity limitation by adding random delays before packet sending

DOI: http://dx.doi.org/10.26583/bit.2021.4.06

Abstract. Attention to covert channels has largely increased due to the documents published by E. Snowden, which described the software and hardware embedding that implement undeclared features of covert information transfer in the Huawei and Juniper network equipment, Apple mobile phones and computers with the Windows XP operating system. A covert channel can be built using any information technology, but often attackers build covert channels in IP networks, since they are widespread, have a high information transfer rate, and ubiquitous information security measures, such as traffic encryption, do not affect the possibility of covert transmission of information via some types of such channels. The limitation of their bandwidth is a promising direction for countering information leakage via network covert channels. This study considers network timing covert channels, provides a method for assessing their capacity, proposes and investigates a way to counter information leakage via such covert channels by introducing noise having added delays before sending packets. The values of the delays are distributed in two different ways: uniformly and according to distribution with a decreasing probability density function. As an experiment, the temporal characteristics of IP traffic from a host in the internal network to a public service were obtained, which were used to verify the obtained methods for assessing the covert channel capacity. A distinctive feature of the calculations is an illustration of the possibility to minimize the load on the communication channel in the context of introducing a countermeasure method, as well as taking into consideration the fact that the intruder's ability to observe the current conditions in the network allows him to adjust the parameters of information transfer to the load in the communication channel, thereby maintaining the maximum possible covert channel bandwidth.

Keywords: covert channels, information leakage, delays, capacity, limitation.
For citation: BELOZUBOVA, Anna I.; KOGOS, Konstantin G.; LEBEDEV, Philipp V. Network covert channels capacity limitation by adding random delays before packet sending. IT Security (Russia), [S.l.], v. 28, n. 4, p. 74–89, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1378. DOI: http://dx.doi.org/10.26583/bit.2021.4.06

Acknowledgement. The research was carried out with support of the Ministry of Science and Higher Education of the Russian Federation (grant for young scientists for research in the area of information security in the digital economy).

Введение

Скрытым каналом называют канал связи, который не предназначался для передачи информации [1]. В ГОСТ Р 53113.1-2008 скрытый канал определяется как канал связи, который может использоваться для нарушения политики информационной безопасности[1]. Проблема утечки информации по сетевым скрытым каналам характеризуется большим масштабом вследствие того, что IP-протокол широко используется и имеет множество функций, позволяющих применять его для скрытой передачи информации.

Обычно скрытые каналы делятся на две группы по технике передачи: скрытые каналы по памяти и по времени[2]. Модификация длины сетевого пакета используется для передачи информации по скрытым каналам по памяти в IP-сетях [2–6]. Внесение изменений в поля заголовков пакетов может служить еще одним примером сетевых

[1]ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.
[2]US Department of Defense (1985) Department of Defense Trusted Computer System Evaluation Criteria. In: US Department of Defense, The ‘Orange Book’ Series.

скрытых каналов по памяти. Для построения скрытых каналов по времени в IP-сетях применяется переупорядочивание пакетов [4] и модификация длин межпакетных интервалов и интенсивности передачи пакетов [7–10].

Среди способов противодействия утечке информации по сетевым скрытым каналам принято выделять обнаружение, устранение и ограничение пропускной способности. Первый способ – обнаружение – позволяет эффективно использовать пропускную способность канала связи. Однако доказано, что нарушитель, который знает параметры системы защиты, может создать необнаруживаемый контролирующим субъектом скрытый канал [11, 12]. Следовательно, обнаружение не обеспечивает полной защиты от утечки информации. Второй способ – устранение – заключается в нормализации параметров IP-трафика. Фиксация длин пакетов, полей заголовков и межпакетных интервалов приводит к устранению скрытого канала, но значительно снижает пропускную способность канала связи. Третий способ – ограничение – дает возможность управляемо уменьшать пропускную способность скрытого канала и, в отличие от предыдущих способов, контролировать остаточную пропускную способность канала коммуникации. Если к защищаемому объекту предъявляются требования информационной безопасности, допускающие функционирование скрытого канала с пропускной способностью не выше заданной, считающейся безопасной, то ограничение пропускной способности скрытых каналов является наиболее подходящей мерой защиты от утечки информации. Такой подход рекомендован в ГОСТ Р 53113.1-2008, авторами TCSEC[3] и специалистами IBM [13]. После реализации метода ограничения необходимо дать оценку остаточной пропускной способности скрытого канала для определения достаточности мер защиты информации от утечки[4].

Скрытые каналы по времени используют временные характеристики сетевого трафика для передачи информации и, соответственно, зависят от состояния сети. Текущую загрузку сети необходимо принимать во внимание при получении значения пропускной способности скрытого канала в условиях отсутствия мер противодействия, которое позволит принять решение о необходимости введения контрмер для снижения пропускной способности скрытого канала до допустимого значения. Авторы исследовали случаи, когда время следования пакета (ВСП) от отправителя к получателю в сети определяется нормальным и экспоненциальным распределениями – наиболее распространенными согласно текущим исследованиям [14–18]. Пропускная способность скрытого канала является функцией от параметров скрытого канала и параметров распределения ВСП. Проведенные исследования показывают, что непринятие в расчет нагрузки на сеть приводит к недооцененности пропускной способности скрытого канала и, как следствие, к ошибкам при построении системы защиты [19, 20].

Исходя из вышеприведенного, была выявлена актуальность исследования метода оценки пропускной способности скрытого канала при введении противодействия и в условиях текущего состояния сети. Статья имеет следующую структуру. Функциональные схемы рассматриваемых сетевых скрытых каналов по времени приведены в разделе 1. В разделе 2 приводятся способы расчета пропускной способности сетевых скрытых каналов. В разделе 3 описывается метод противодействия утечке информации. В разделах 4 и 5

[3]US Department of Defense (1985) Department of Defense Trusted Computer System Evaluation Criteria. In: US Department of Defense, The ‘Orange Book’ Series. Palgrave Macmillan, London.

[4]ГОСТ Р 53113.2-2009. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.

даны способы оценки пропускной способности скрытых каналов в условиях введения метода противодействия в случаях экспоненциального и нормального распределения ВСП. Обзор результатов и общие выводы представлены в разделе 6.

1. Сетевые скрытые каналы по времени

Для исследования в работе выбраны два сетевых скрытых канала по времени: основанный на изменении интенсивности передачи пакетов (on/off скрытый канал) и длин межпакетных интервалов. Далее считается, что передаваемые по скрытому каналу биты «0» и «1» передаются с разными вероятностями: $p_{\text{вх}}(0) = q, p_{\text{вх}}(1) = 1 - q.$ Для верификации полученных формул, использующихся в расчетах пропускных способностей скрытых каналов, авторы исследовали локальную сеть с одним роутером, утилита ping использовалась для получения времени следования более 10 тысяч IP-пакетов. Считается, что ВСП составляет половину значения RTT.

1.1 On/off скрытый канал

Участники скрытого информационного обмена выбирают длительность интервала t, в который отправитель либо передает один пакет, либо бездействует, чтобы отправить «1» или «0» соответственно. Для декодирования информации получатель фиксирует: получил он пакет в течение интервала времени t или нет. При этом для обеспечения высокой скорости передачи информации и снижения уровня ошибок в скрытом канале длина интервала t может меняться. На рис. 1 приведен пример передачи сообщения с использованием скрытого канала.

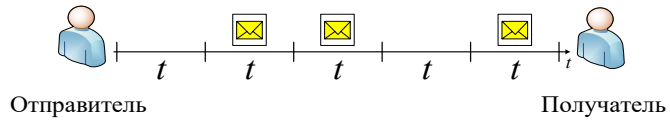

Рис. 1. Пример функционирования on/off скрытого канала: передача сообщения «01101»
Fig. 1. Sending message «01101» via on/off covert channel

1.2 Сетевой скрытый канал, основанный на изменении длин межпакетных интервалов

Участники скрытого информационного обмена выбирают длительность интервалов t_0 и t_1, с которыми отправитель передает пакеты, чтобы отправить «0» и «1» соответственно. Аналогично, для поддержания высокой скорости передачи информации и снижения уровня ошибок в скрытом канале значения параметров t_0 и t_1 могут меняться. На рис. 2 приведен пример передачи сообщения с использованием скрытого канала.

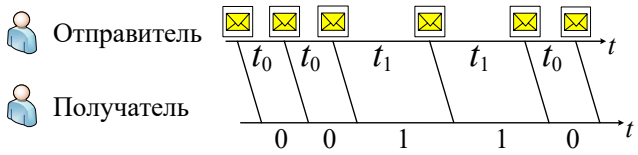

Рис. 2. Пример функционирования скрытого канала, основанного на изменении длин межпакетных интервалов: передача сообщения «00110»
Fig. 2. Sending message «00110» via covert channel based on interpacket intervals modulation

Обозначим длину интервала между приемами пакетов как $t_{\text{инт}}$, а пограничное значение длины межпакетного интервала для определения передаваемого символа как $t_{\text{гр}} = \frac{t_0 + t_1}{2}$. Для декодирования бита «0» должно выполняться условие $t_{\text{инт}} \le t_{\text{гр}}$, в обратном случае получатель декодирует бит «1».

2. Пропускная способность скрытых каналов с ошибками

Пропускную способность скрытого канала с ошибками можно оценить по следующей формуле:

$$C = \max_{X} \frac{I(X,Y)}{T + \mu}, \tag{1}$$

где I – взаимная информация случайных величин X, Y, описывающих входные и выходные характеристики скрытого канала, T – среднее время передачи пакетов, μ – среднее время, требуемое для перемещения пакета в канал передачи данных. Для оценки взаимной информации используется формула:

$$I(X,Y) = H(Y) - H(Y \mid X), \tag{2}$$

для оценки энтропии Y используется формула:

$$H(Y) = -\sum_{y \in \{0,1\}} p_{\text{вых}}(y) \log_2 p_{\text{вых}}(y), \tag{3}$$

условная энтропия Y относительно X равна:

$$H(Y \mid X) = -\sum_{x \in \{0,1\}} p_{\text{вх}}(x) \sum_{y \in \{0,1\}} p(y \mid x) \log_2 p(y \mid x), \tag{4}$$

где $p_{\text{вых}}(i)$ вероятность распознавания символа «i», $p(i \mid j)$ – вероятность распознавания символа «i», при отправке символа «j», $i, j \in \{0,1\}$. Для расчета пропускной способности on/off скрытого канала используется формула:

$$C = \max_{q,t} \left\{ -\frac{q \log_2 q + (1-q) \log_2 (1-q)}{t + \mu} \right\}. \tag{5}$$

Для расчета пропускной способности скрытого канала, основанного на изменении длин межпакетных интервалов, используется формула:

$$C = \max_{q,t_0,t_1} \left(-\frac{q \log_2 q + (1-q) \log_2 (1-q)}{t_{\text{гр}} + \mu} \right). \tag{6}$$

Далее в качестве противодействия утечке информации по скрытым каналам рассматривается метод на основе введения шума в скрытый канал, и описывается способ оценки остаточной пропускной способности скрытого канала, учитывающий способности атакующего правильно настроить параметры скрытого канала.

3. Метод противодействия

Предлагаемый метод противодействия заключается во введении перед отправкой пакетов дополнительных задержек τ, $\tau \in (0;d)$, где d – параметр противодействия. Таким образом в скрытый канал добавляется шум, что приводит к ошибкам и, как следствие, снижает его пропускную способность. Исследуется два класса распределения значений задержек:

- равномерное распределение на интервале $(0;d)$;
- распределение на интервале $(0;d)$ с невозрастающей функцией плотности распределения вероятности.

Решая задачу снижения пропускной способности скрытого канала до допустимого значения, авторы дополнительно рассматривают распределение с невозрастающей функцией плотности, которое может обеспечить снижение нагрузки на канал связи по сравнению со способом, когда значения задержек выбираются по равномерному закону распределения на некотором интервале. Это обуславливается тем, что малые величины задержек будут генерироваться чаще [21]. В качестве примера функции распределения из второго класса в работе рассматривается бета-распределение с функцией плотности распределения вероятности, имеющей вид:

$$f(x) = \frac{1}{B(\alpha,\beta)} x^{\alpha-1}(1-x)^{\beta-1}, \tag{7}$$

где $\alpha, \beta > 0$ параметры распределения, и $B(\alpha,\beta) = \int_0^1 x^{\alpha-1}(1-x)^{\beta-1}dx$. На рис. 3 приведены графики плотности распределения вероятности для различных значений параметров α, β бета-распределения.

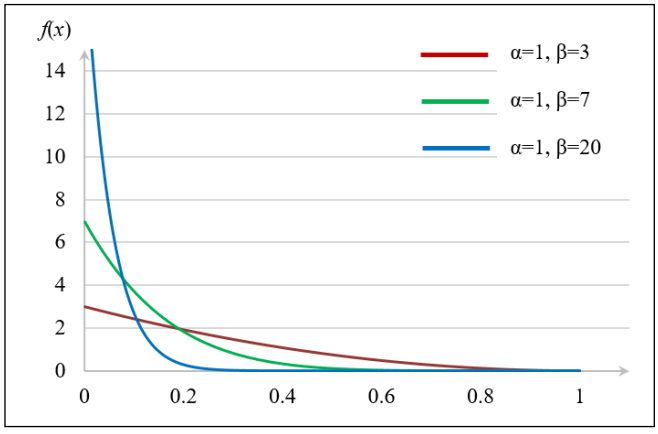

Рис. 3. Графики плотности вероятности бета-распределения
Fig. 3. Probability density plots of beta distribution

При принятии решения о выборе способа генерации задержек и его параметрах необходимо провести расчеты остаточной пропускной способности скрытого канала и канала связи, чтобы определить, как выбор того или иного вида распределения значений задержек влияет на уровень нагрузки на канал связи, и тем самым обеспечить эффективное использование коммуникационного канала.

3.1 Противодействие утечке информации по on/off скрытому каналу

Для on/off скрытого канала введение задержек может приводить к тому, что отправленный в определенном интервале времени *t* IP-пакет придет на стороне получателя в следующем временном интервале.

На рис. 4 показана отправка сообщения «01011», и введение задержки τ перед отправкой первого пакета, которое приводит к «переносу» пакета в следующий интервал времени *t*, в результате чего отправитель декодирует сообщение «00111».

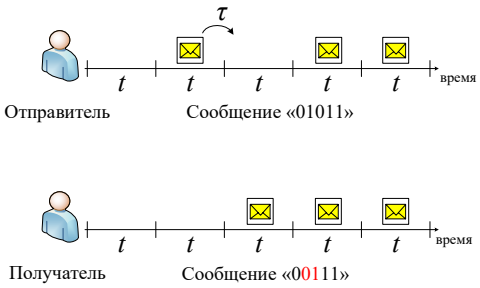

Рис. 4. Введение задержек перед отправкой пакетов
Fig. 4. Introducing delays before packet sending

3.2 Противодействие утечке информации по скрытому каналу, основанному на изменении длин межпакетных интервалов

Ошибки в скрытом канале, основанном на изменении длин межпакетных интервалов, заключаются в том, что задержки, введенные перед отправкой пакетов, изменяют длины межпакетных интервалов на стороне получателя. Таким образом межпакетные интервалы, соответствующие биту «0», могут увеличиваться до длины, соответствующей биту «1», и наоборот [21].

На рис. 5 показана отправка сообщения «0101» в скрытом канале, на рис. 6 – отправка того же сообщения и проиллюстрировано появление ошибок и распознавание получателем сообщения «1001» в результате введения задержки τ перед отправкой второго пакета.

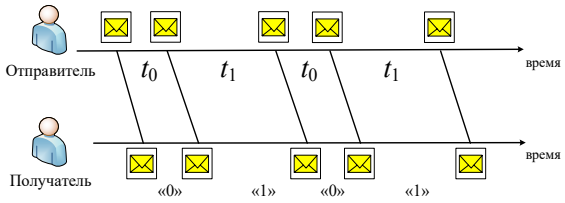

Рис. 5. Отправка сообщения «0101» в скрытом канале без введения метода противодействия
Fig. 5. Sending message "0101" via the covert channel without counteraction method

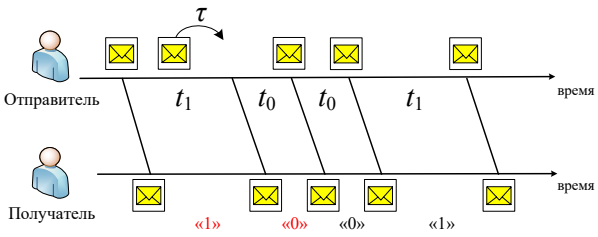

Рис. 6. Появление ошибок в скрытом канале из-за введения задержек перед отправкой пакетов
Fig. 6. Appearance of errors in the covert channel due to delay introduction before packet sending

4. Остаточная пропускная способность канала, когда время передачи пакета определено экспоненциальным распределением

Рассмотрим $f(x)$ – функцию распределения ВСП. Согласно исследованиям $f(x)$ может принимать форму экспоненциального, нормального, усеченного нормального, гамма, логнормального, закона распределения и их различных сумм и распределения Вейбулла [14–18]. Пусть функция $f(x)$ описывается экспоненциальным законом распределения с функцией плотности вероятности:

$$f(x) = \lambda e^{-\lambda x}, \tag{8}$$

и функцией распределения:

$$F = 1 - e^{-\lambda x}. \tag{9}$$

4.1.1 Остаточная пропускная способность on/off скрытого канала

Передача пакета не происходит мгновенно, поэтому момент нового интервала t на стороне получателя можно сдвинуть вперед на значение $t_{\min}$, чтобы не ждать обнаружения пакета в течение интервала времени, во время которого пакет будет обрабатываться на сетевых устройствах и передаваться по каналу связи. Таким образом, вероятности p_{no} прибытия IP-пакета в пределах предполагаемого интервала времени t и p_{yes} – в интервале времени t, следующем за интервалом, в котором был отправлен пакет, определяются условиями, приведенными в табл. 1.

Таблица 1. Условия определения вероятностей p_{no} и p_{yes}

Вероятность	Неравенство
p_{no}	$t_{\text{след}} + \tau - t_{\min} < t$ $t_{\text{след}} < t + t_{\min} - \tau$
p_{yes}	$t_{\text{след}} + \tau - t_{\min} \geq t$ $t_{\text{след}} \geq t + t_{\min} - \tau$

Для определения вероятности p_{no} необходимо определить вероятность того, что неравенство $t_{\text{след}} < t + t_{\min} - \tau$ соблюдается, где $t_{\text{след}}$ и $t_{\min}$ – величины, подчиняющиеся экспоненциальному закону распределения. Следовательно

$$\begin{aligned} p_{\text{no}} &= F(t + t_{\min} - \tau) = 1 - e^{-\lambda(t + t_{\min} - \tau)}, \\ p_{\text{yes}} &= 1 - p_{\text{no}}. \end{aligned} \tag{10}$$

Чтобы определить условные вероятности распознавания символа «*y*», при отправке символа «*x*», необходимо рассмотреть, как изменения времени следования пакетов в сети влияют на детектирование моментов прибытия пакетов получателем. На рис. 7–10 показаны события отправки и прибытия пакетов, соответствующие условным вероятностям распознавания выходных символов. Конверт означает, что пакет был отправлен в интервале времени t, символ “—” означает, что пакет не был отправлен в интервале времени t, символ «*» означает, что пакет может быть отправлен или не быть отправлен на стороне получателя или может быть получен или не быть получен на стороне получателя в интервале времени t, стрелкой обозначается следование пакета и момент его прибытия на стороне получателя: в том же интервале времени t, в котором пакет был отправлен, или в следующем.

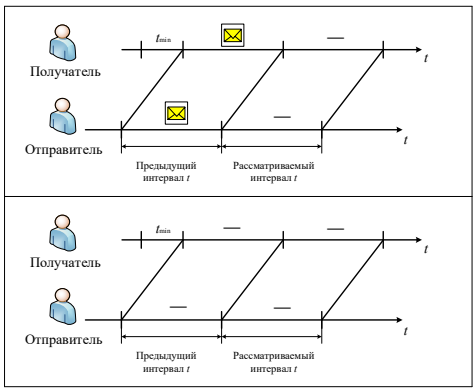

Рис. 7. Варианты следования пакетов, соответствующие условной вероятности p(0|0)
Fig. 7. Packet transfers corresponding to conditional possibility p(0|0)

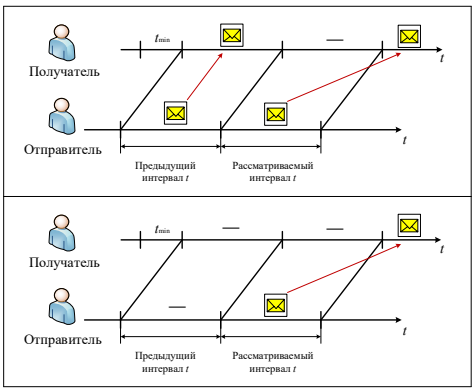

Рис. 8. Варианты следования пакетов, соответствующие условной вероятности p(0|1)
Fig. 8. Packet transfers corresponding to conditional possibility p(0|1)

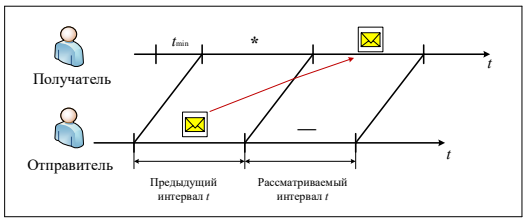

Рис. 9. Варианты следования пакетов, соответствующие условной вероятности p(1|0)
Fig. 9. Packet transfers corresponding to conditional possibility p(1|0)

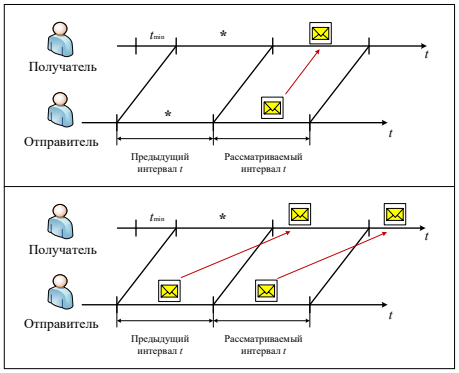

Рис. 10. Варианты следования пакетов, соответствующие условной вероятности p(1|1)
Fig. 10. Packet transfers corresponding to conditional possibility p(1|1)

Следовательно, условные вероятности определяются следующим образом:

$$\begin{aligned} p(0\,|\,0) &= (1-q)\,p_{\text{no}} + q, \\ p(1\,|\,0) &= 1 - p(0\,|\,0), \\ p(0\,|\,1) &= (1-q)\,p_{\text{no}}\,p_{\text{yes}} + qp_{\text{yes}}, \\ p(1\,|\,1) &= 1 - p(0\,|\,1). \end{aligned} \tag{11}$$

В этом случае вероятности того, что получатель в скрытом канале декодирует символы «0» и «1», определяются по формулам:

$$\begin{aligned} p_{\text{вых}}(0) &= qp(0\,|\,0) + (1-q)\,p(0\,|\,1), \\ p_{\text{вых}}(1) &= qp(1\,|\,0) + (1-q)\,p(1\,|\,1). \end{aligned} \tag{12}$$

Пропускная способность скрытого канала определяется по формулам (1) и (2).

4.2 Остаточная пропускная способность скрытого канала, основанного на изменении длин межпакетных интервалов

Длина межпакетного интервала определяется как разница между временем прибытия к получателю двух IP-пакетов подряд. Пусть такие IP-пакеты обозначаются «первый» и «второй». Тогда вводятся следующие обозначения:

– $t_{\text{п}}$ – время передачи «первого» IP-пакета,

– $t_{\text{в}}$ – время передачи «второго» IP-пакета.

В табл. 2 приведены неравенства, определяющие условные вероятности $p(y|x)$ распознавания символа «y» при отправке символа «x» при введении задержек перед отправкой пакетов.

Таблица 2. Определение условных вероятностей

Условная вероятность	Неравенство
$p(0\|0)$	$t_0 - t_{\text{п}} + t_{\text{в}} - \tau_{\text{п}} + \tau_{\text{в}} \le t_{\text{гр}}$
$p(0\|1)$	$t_1 - t_{\text{п}} + t_{\text{в}} - \tau_{\text{п}} + \tau_{\text{в}} \le t_{\text{гр}}$
$p(1\|0)$	$t_0 - t_{\text{п}} + t_{\text{в}} - \tau_{\text{п}} + \tau_{\text{в}} \ge t_{\text{гр}}$
$p(1\|1)$	$t_1 - t_{\text{п}} + t_{\text{в}} - \tau_{\text{п}} + \tau_{\text{в}} \ge t_{\text{гр}}$

Пусть $z = t_{\text{в}} - t_{\text{п}}$, где $t_{\text{п}}$ и $t_{\text{в}}$ – случайные величины, подчиняющиеся экспоненциальному закону распределения, тогда функция плотности распределения вероятности величины z равна:

$$f(z) = \int_{-\infty}^{+\infty} f(x) f(x-z) dx = \int_{-\infty}^{+\infty} \lambda e^{-\lambda x} \lambda e^{-\lambda(x-z)} dx = \begin{cases} \frac{\lambda}{2} e^{\lambda z}, z \le 0, \\ \frac{\lambda}{2} e^{-\lambda z}, z > 0. \end{cases} \quad (13)$$

Тогда условные вероятности распознавания символов в скрытом канале равны:

$$\begin{aligned} p(0\,|\,0) &= \int_{-\infty}^{t_{\text{гр}} - t_0 + \tau_{\text{п}} - \tau_{\text{в}}} f(z) dz = 1 - \frac{1}{2} e^{-\lambda(t_{\text{гр}} - t_0 + \tau_{\text{п}} - \tau_{\text{в}})}, \\ p(0\,|\,1) &= \int_{-\infty}^{t_{\text{гр}} - t_1 + \tau_{\text{п}} - \tau_{\text{в}}} f(z) dz = 1 - \frac{1}{2} e^{-\lambda(t_{\text{гр}} - t_1 + \tau_{\text{п}} - \tau_{\text{в}})}, \\ p(1\,|\,0) &= \int_{t_{\text{гр}} - t_0 + \tau_{\text{п}} - \tau_{\text{в}}}^{+\infty} f(z) dz = \frac{1}{2} e^{-\lambda(t_{\text{гр}} - t_0 + \tau_{\text{п}} - \tau_{\text{в}})}, \\ p(1\,|\,1) &= \int_{t_{\text{гр}} - t_1 + \tau_{\text{п}} - \tau_{\text{в}}}^{+\infty} f(z) dz = \frac{1}{2} e^{-\lambda(t_{\text{гр}} - t_1 + \tau_{\text{п}} - \tau_{\text{в}})}. \end{aligned} \quad (14)$$

При этом вероятности того, что получатель в скрытом канале декодирует символы «0» и «1», определяются по формулам (8)**Ошибка! Источник ссылки не найден.**. При п омощи формул (1) и (2) определяется пропускная способность скрытого канала.

5. Остаточная пропускная способность канала, когда время передачи пакета определено нормальным распределением

Пусть функция $f(x)$ описывается нормальным законом распределения с функцией плотности вероятности:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-(x-\mu)^2}{2\sigma^2}}, \quad (15)$$

и функцией распределения:

$$F = \frac{1}{2}\left[1 + erf\left(\frac{x-\mu}{\sqrt{2\sigma^2}}\right)\right],$$
$$erf(m) = \frac{2}{\sqrt{\pi}}\int_0^m e^{-t^2}dt, \quad (16)$$

где *erf*(*x*) – функция ошибок (функция Лапласа).

5.1 Остаточная пропускная способность on/off скрытого канала

Как и в предыдущем случае, вероятности p_{no} и p_{yes} определяются условиями, приведенными в табл. 1, и для определения вероятности p_{no} необходимо определить вероятность того, что соблюдается неравенство $t_{\text{след}} < t + t_{\min} - \tau$, где $t_{\text{след}}$ и $t_{\min}$ – величины, описываемые нормальным законом распределения. Следовательно

$$p_{\text{no}} = F(t + t_{\min} - \tau) = \frac{1}{2}\left[1 + erf\left(\frac{t + t_{\min} - \tau - \mu}{\sqrt{2\sigma^2}}\right)\right],$$
$$p_{\text{yes}} = 1 - p_{\text{no}}. \quad (17)$$

На рис. 7 показана отправка пакетов и их «перенос», соответствующие условным вероятностям выходных символов. Условные вероятности $p(y|x)$ определяются по формулам (7), вероятности того, что получатель в скрытом канале декодирует символы «0» и «1», определяются формулами (8). Пропускная способность скрытого канала определяется по формулам (1) и (2).

Используя полученные формулы и перебор параметров скрытого канала и метода противодействия, можно оценить наибольшее значение остаточной пропускной способности канала при введении задержек перед отправкой пакета, значения которых распределены равномерно и согласно убывающему закону распределения. На рис. 11 и рис. 12 представлены графики зависимости пропускной способности скрытого канала при введении задержек перед отправкой пакетов от параметра противодействия.

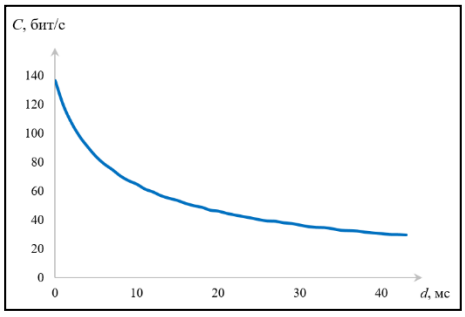

Рис. 11. График зависимости остаточной пропускной способности on/off скрытого канала от параметра противодействия d при генерации значений задержек по равномерному распределению
Fig. 11. The residual on/off channel capacity as function of the countermeasure parameter d when generating delays on a uniform distribution

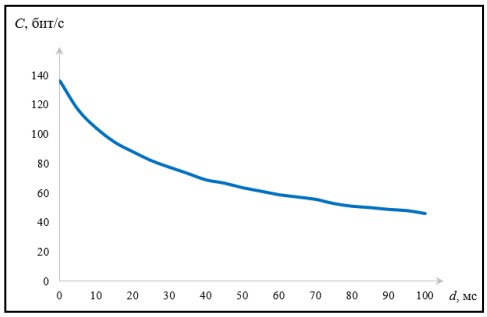

Рис. 12. График зависимости остаточной пропускной способности on/off скрытого канала от параметра противодействия d при генерации значений задержек по бета-распределению
Fig. 12. The residual on/off channel capacity as function of the countermeasure parameter d when generating delays on a beta distribution

После определения значения параметра метода противодействия *d*, позволяющего снизить пропускную способность скрытого канала до значения $C_{\text{доп}}$, необходимо рассмотреть возможности, позволяющие снизить нагрузку на канал связи, создающуюся

введением задержек. На рис. 13 показан график зависимости остаточной пропускной способности скрытого канала от остаточной пропускной способности канала связи $V_{ост}$ при генерации значений задержек двумя различными способами.

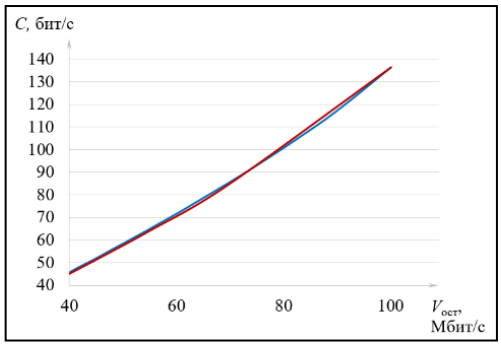

Рис. 13. График зависимости остаточной пропускной способности on/off скрытого канала от остаточной пропускной способности канала связи в условиях генерации задержек перед отправкой пакетов для двух способов генерации задержек
Fig. 13. The residual on/off channel capacity as function of the residual communication channel capacity under the conditions of generating delays before sending packets for two delay generating methods

На графике показана зависимость остаточной пропускной способности скрытого канала в условиях генерации задержек перед отправкой пакетов от остаточной пропускной способности канала связи для двух распределений значений задержек: равномерное на интервале $(0;d)$ и бета-распределение с параметрами $\alpha = 1, \beta = 7$. Как видно из графика, оба способа генерации задержек оказывают практически одинаковую нагрузку на канал связи. Однако, в условиях распределения трафика в сети отличных, от рассматриваемых в данном подразделе, разница в снижении $V_{ост}$ может оказаться существеннее. В связи с этим рекомендуется осуществлять данную проверку для определения возможностей минимизации неэффективного использования пропускной способности коммуникационного канала.

5.2 Скрытый канал, основанный на изменении длин межпакетных интервалов

Как и в предыдущем случае, условная вероятность распознавания символов в скрытом канале определяется при исследовании условий, приведенных в табл. 2. Пусть $z = t_в - t_п$, где $t_п$ и $t_в$ – случайные величины, подчиняющиеся нормальному закону распределения. Тогда:

$$\begin{aligned}
p(0\,|\,0) &= \int_{-\infty}^{t_{гр}-t_0+d_п-d_в} f(z)dz = F'(t_{гр}-t_0+d_п-d_в),\\
p(0\,|\,1) &= \int_{-\infty}^{t_{гр}-t_1+d_п-d_в} f(z)dz = F'(t_{гр}-t_1+d_п-d_в),\\
p(1\,|\,0) &= \int_{t_{гр}-t_0+d_п-d_в}^{+\infty} f(z)dz = 1-F'(t_{гр}-t_0+d_п-d_в),\\
p(1\,|\,1) &= \int_{t_{гр}-t_1+d_п-d_в}^{+\infty} f(z)dz = 1-F'(t_{гр}-t_1+d_п-d_в).
\end{aligned} \qquad (18)$$

При этом вероятности того, что получатель в скрытом канале декодирует символы «0» и «1», определяются по формулам (8). И при помощи формул (1) и (2) определяется пропускная способность скрытого канала.

Используя полученные формулы и перебор параметров скрытого канала и метода противодействия, можно оценить наибольшее значение остаточной пропускной способности канала при введении задержек перед отправкой пакета, значения которых распределены равномерно и согласно убывающему закону распределения. На рис. 14 и рис. 15 представлены графики зависимости пропускной способности скрытого канала при введении задержек перед отправкой пакетов от параметра противодействия.

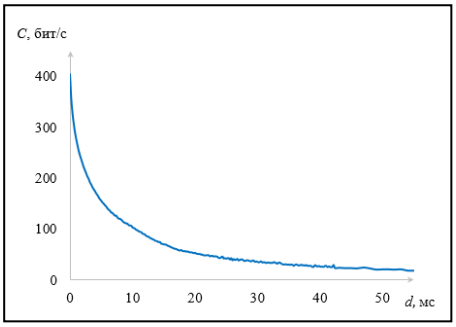

Рис. 14. График зависимости остаточной пропускной способности скрытого канала, основанного на изменении длин межпакетных интервалов, от параметра противодействия d при генерации значений задержек по равномерному распределению

Fig. 14. The residual capacity of the covert channel based on interpacket intervals modulation as function of the countermeasure parameter d when generating delays on a uniform distribution

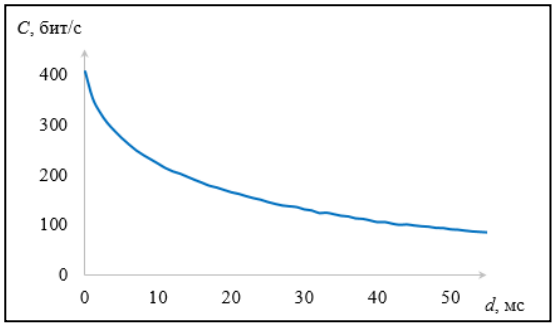

Рис. 15. График зависимости остаточной пропускной способности скрытого канала, основанного на изменении длин межпакетных интервалов, от параметра противодействия d при генерации значений задержек по бета-распределению

Fig. 15. The residual capacity of the covert channel based on interpacket intervals modulation as function of the countermeasure parameter d when generating delays on a beta distribution

Аналогично предыдущему пункту рассмотрим возможности по снижению нагрузки на канал связи, создающуюся введением задержек. Ниже на рис. 16 показан график зависимости остаточной пропускной способности скрытого канала от остаточной пропускной способности канала связи $V_{ост}$ при генерации значений задержек двумя различными способами.

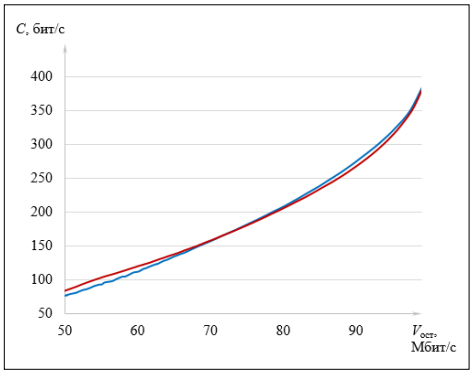

Рис. 16. График зависимости остаточной пропускной способности скрытого канала, основанного на изменении длин межпакетных интервалов, от остаточной пропускной способности канала связи в условиях генерации задержек перед отправкой пакетов для различных способов генерации задержек

Fig. 16. The residual capacity of the covert channel based on interpacket intervals modulation as function of the residual communication channel capacity under the conditions of generating delays before sending packets for two delay generating methods

На графике показана зависимость остаточной пропускной способности скрытого канала в условиях генерации задержек перед отправкой пакетов от остаточной пропускной способности канала связи для двух распределений значений задержек: равномерное на интервале (0;d) и бета-распределение с параметрами $\alpha = 1, \beta = 7$. Как видно из графика, при снижении пропускной способности скрытого канала до значения, $C_{\text{доп}}$=100 б/с преимущество имеет способ генерации задержек перед отправкой пакетов по бета-распределению, так как в таком случае нагрузка на канал связи ниже, что позволит сохранить большую остаточную пропускную способность канала связи по сравнению с генерацией равномерно распределенных значений задержек.

Заключение

В работе предложен и исследован способ ограничения пропускной способности скрытого канала путем введения дополнительных случайных задержек перед отправкой пакетов. Изучены два сетевых скрытых канала по времени: каналы, основанные на изменении интенсивности передачи пакетов и длин межпакетных интервалов. Учет возможностей нарушителя проводить настройку параметров скрытого канала, приводящую к увеличению его пропускной способности, стал возможен благодаря определению распределения времени следования пакетов в канале между участниками коммуникации. Предложенный метод введения дополнительных случайных задержек перед отправкой пакетов отличается тем, что он применим в случае, когда к защищаемому объекту предъявляются требования информационной безопасности, допускающие функционирование скрытого канала с пропускной способностью не выше заданной. Отличительной особенностью предложенного метода является генерация значений задержек, распределенных различным образом. Разработан способ оценки остаточной пропускной способности скрытых каналов при введении метода противодействия, а также приведены рекомендации по выбору способа генерации значений задержек с целью минимизации нагрузки на канал связи. Показано, что в некоторых случаях выбор значений задержек, которые подчиняются распределению с убывающей функцией плотности вероятности, может снизить нагрузку на коммуникационный канал.

СПИСОК ЛИТЕРАТУРЫ:

1. Lampson B.W. A Note on the Confinement Problem. Communications of the ACM. Vol. 16, no. 10, 1973. P. 613–615. DOI: http://dx.doi.org/10.1145/362375.362389.
2. Ahsan K., Kundur D. Practical Data Hiding in TCP/IP. Proceedings of the ACM Workshop on Multimedia Security, 2002. URL: https://www.researchgate.net/publication/2878386_Practical_data_hiding_in_TCPIP (дата обращения: 01.08.2021).
3. Zander S., Armitage G., Branch B. Covert Channels in the IP Time To Live Field. Proceedings of the Australian Telecommunication Networks and Applications Conference, 2006. URL: https://www.researchgate.net/publication/228875924_Covert_channels_in_the_IP_time_to_live_field (дата обращения: 01.08.2021).
4. Zander S., Armitage G., Branch P. A Survey of Covert Channels and Countermeasures in Computer Network Protocols. IEEE Communications Surveys and Tutorials. Vol. 9, no. 3, 2007. P. 44–57. DOI: http://dx.doi.org/10.1109/COMST.2007.4317620.
5. Epishkina A., Kogos K. A random traffic padding to limit packet size covert channels. Proceedings of the 2015 Federated Conference on Computer Science and Information Systems. Vol. 5, 2015. P. 1107–1113. DOI: http://dx.doi.org/10.15439/2015F88.
6. Epishkina A., Kogos K. Covert channels parameters evaluation using the information theory statements. Proceedings of the 5th International Conference on IT convergence and security. 2015. P. 395–399. DOI: http://dx.doi.org/10.1109/ICITCS.2015.7292966.
7. Cabuk S., Brodley C.E., Shields C. IP covert timing channels: design and detection. Proceedings of the eleventh ACM conference on computer and communications security. 2004. P. 178–187. DOI: http://dx.doi.org/10.1145/1030083.1030108.

8. Girling C.G. Covert channels in LAN's. IEEE Transactions on software engineering. Vol. 13, no. 2, 1987. P. 292–296. DOI: http://dx.doi.org/10.1109/COMST.2007.4317620.
9. Shah G., Molina A., Blaze M. Keyboards and Covert Channels. Proceedings of the 15th USENIX Security Symposium, 2006. P. 59–75. URL: https://www.researchgate.net/publication/234829288_Keyboards_and_Covert_Channels (дата обращения: 01.08.2021).
10. Sellke S.H., Wang C.-C., Bagchi S., Shroff N.B. Covert TCP/IP timing channels: theory to implementation. Proceedings of the 28th conference on computer communications. 2009. P. 2204–2212. DOI: http://dx.doi.org/10.1109/INFCOM.2009.5062145.
11. Грушо А.А. Скрытые каналы и безопасность информации в компьютерных системах // Дискретная математика. 1998. Т. 10, вып.1. С. 3–9. DOI: https://doi.org/10.4213/dm411.
12. Грушо А.А. О существовании скрытых каналов. Дискретная математика. 1999. Т. 11, вып. 1. С. 24–28. DOI: https://doi.org/10.4213/dm363.
13. IBM Knowledge Center. URL: https://www.ibm.com/support/knowledgecenter/ssw_aix_71/security/taix_audit_bandwidth.html (дата обращения: 29.06.2021).
14. Elteto T., Molnar S. On the distribution of round-trip delays in TCP/IP networks. Proceedings of the 24th Conference on Local Computer Networks lcn'99. 1999. DOI: http://dx.doi.org/10.1109/LCN.1999.802014.
15. Karakas M. Determination of network delay distribution over the internet. Thesis submitted to the graduate school of natural and applied sciences of the middle east technical university, December 2003. URL: https://www.semanticscholar.org/paper/De-Jitter-Buffer-Role-in-Improving-VOIP-Connection-Lebl-Mileusnić/69408025b0dfce8a24e21d54893ce2c8d627146b (дата обращения: 01.08.2021).
16. Sukhov A.M., Kuznetsova N.Yu. What type of distribution for packet delay in a global network should be used in the control theory? 2019. URL: https://www.researchgate.net/publication/45864214_What_type_of_distribution_for_packet_delay_in_a_global_network_should_be_used_in_the_control_theory (дата обращения: 01.08.2021).
17. Sagatov E.S., Samoilova D.V., Sukhov A.M. Composite distribution for one-way packet delay in the global network, 24th Telecommunications forum TELFOR 2016. DOI: http://dx.doi.org/10.1109/TELFOR.2016.7818726.
18. Sukhov A.M., Kuznetsova N.Yu., Pervitsky A.K., Galtsev A.A. Generating Function For Network Delay. Journal of High Speed Networks. Vol. 22, no. 4. P. 321–333, 2016. DOI: http://dx.doi.org/10.3233/JHS-160552.
19. Belozubova A., Epishkina A., Kogos K. How to limit capacity of timing covert channel by adding extra delays. Procedia Computer Science. 2021. DOI: http://dx.doi.org/10.1016/j.procs.2021.06.008.
20. Belozubova A., Epishkina A., Kogos K. On/off covert channel capacity limitation by adding extra delays. ElConRus 2021. 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering. P. 2318–2322. DOI: http://dx.doi.org/10.1109/ElConRus51938.2021.9396545.
21. Белозубова А.И., Епишкина А.В., Когос К.Г. О введении задержек для противодействия утечке информации по скрытым каналам в IP-сетях. Методы и технические средства обеспечения безопасности информации. 2019, № 28. С. 81–82. URL: https://elibrary.ru/item.asp?id=38251172.

REFERENCES:

[1] Lampson B.W. A Note on the Confinement Problem. Communications of the ACM. Vol. 16, no. 10, 1973. P. 613–615. DOI: http://dx.doi.org/10.1145/362375.362389.
[2] Ahsan K., Kundur D. Practical Data Hiding in TCP/IP. Proceedings of the ACM Workshop on Multimedia Security, 2002. URL: https://www.researchgate.net/publication/2878386_Practical_data_hiding_in_TCPIP (accessed: 01.08.2021).
[3] Zander S., Armitage G., Branch B. Covert Channels in the IP Time To Live Field. Proceedings of the Australian Telecommunication Networks and Applications Conference, 2006. URL: https://www.researchgate.net/publication/228875924_Covert_channels_in_the_IP_time_to_live_field (accessed: 01.08.2021).
[4] Zander S., Armitage G., Branch P. A Survey of Covert Channels and Countermeasures in Computer Network Protocols. IEEE Communications Surveys and Tutorials. Vol. 9, no. 3, 2007. P. 44–57. DOI: http://dx.doi.org/10.1109/COMST.2007.4317620.
[5] Epishkina A., Kogos K. A random traffic padding to limit packet size covert channels. Proceedings of the 2015 Federated Conference on Computer Science and Information Systems. Vol. 5, 2015. P. 1107–1113. DOI: http://dx.doi.org/10.15439/2015F88.
[6] Epishkina A., Kogos K. Covert channels parameters evaluation using the information theory statements. Proceedings of the 5th International Conference on IT convergence and security. 2015. P. 395–399. DOI: http://dx.doi.org/10.1109/ICITCS.2015.7292966.

[7] Cabuk S., Brodley C.E., Shields C. IP covert timing channels: design and detection. Proceedings of the eleventh ACM conference on computer and communications security. 2004. P. 178–187. DOI: http://dx.doi.org/10.1145/1030083.1030108.

[8] Girling C.G. Covert channels in LAN's. IEEE Transactions on software engineering. Vol. 13, no. 2, 1987. P. 292–296. DOI: http://dx.doi.org/10.1109/COMST.2007.4317620.

[9] Shah G., Molina A., Blaze M. Keyboards and Covert Channels. Proceedings of the 15th USENIX Security Symposium, 2006. P. 59–75. URL: https://www.researchgate.net/publication/234829288_Keyboards_ and_Covert_Channels (accessed: 01.08.2021).

[10] Sellke S.H., Wang C.-C., Bagchi S., Shroff N.B. Covert TCP/IP timing channels: theory to implementation. Proceedings of the 28th conference on computer communications. 2009. P. 2204–2212. DOI: http://dx.doi.org/10.1109/INFCOM.2009.5062145.

[11] Grusho A.A. Hidden channels and information security in computer systems. Diskr. Mat. 1998. Vol. 10, Issue 1. S. 3–9. DOI: https://doi.org/10.4213/dm411 (in Russian).

[12] Grusho A.A. On the existence of hidden channels. Diskr. Mat. 1999. Vol. 11, Issue 1. P. 24–28. DOI: https://doi.org/10.4213/dm363

[13] IBM Knowledge Center. URL: https://www.ibm.com/support/knowledgecenter/ssw_aix_71/security/taix_audit_bandwidth.html (accessed: 29.06.2021).

[14] Elteto T., Molnar S. On the distribution of round-trip delays in TCP/IP networks. Proceedings of the 24th Conference on Local Computer Networks lcn'99. 1999. DOI: http://dx.doi.org/10.1109/LCN.1999.802014.

[15] Karakas M. Determination of network delay distribution over the internet. Thesis submitted to the graduate school of natural and applied sciences of the middle east technical university, December 2003. URL: https://www.semanticscholar.org/paper/De-Jitter-Buffer-Role-in-Improving-VOIP-Connection-Lebl-Mileusnić/69408025b0dfce8a24e21d54893ce2c8d627146b (accessed: 01.08.2021).

[16] Sukhov A.M., Kuznetsova N.Yu. What type of distribution for packet delay in a global network should be used in the control theory? 2019. URL: https://www.researchgate.net/publication/45864214_What_type_of_distribution_for_packet_delay_in_a_global_network_should_be_used_in_the_control_theory (accessed: 01.08.2021).

[17] Sagatov E.S., Samoilova D.V., Sukhov A.M. Composite distribution for one-way packet delay in the global network, 24th Telecommunications forum TELFOR 2016. DOI: http://dx.doi.org/10.1109/TELFOR.2016.7818726.

[18] Sukhov A.M., Kuznetsova N.Yu., Pervitsky A.K., Galtsev A.A. Generating Function For Network Delay. Journal of High Speed Networks. Vol. 22, no. 4. P. 321–333, 2016. DOI: http://dx.doi.org/10.3233/JHS-160552.

[19] Belozubova A., Epishkina A., Kogos K. How to limit capacity of timing covert channel by adding extra delays. Procedia Computer Science. 2021 г. DOI: http://dx.doi.org/10.1016/j.procs.2021.06.008.

[20] Belozubova A., Epishkina A., Kogos K. On/off covert channel capacity limitation by adding extra delays. ElConRus 2021. 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering. P. 2318–2322. DOI: http://dx.doi.org/10.1109/ElConRus51938.2021.9396545.

[21] Belozubova A., Epishkina A., Kogos K. About delays insertion for information leakage counteraction via IP covert channels. Methods and Technical Means of Information Security. 2019, no. 28. P. 81–82. URL: https://elibrary.ru/item.asp?id=38251172 (accessed: 01.08.2021) (in Russian).

Поступила в редакцию – 3 августа 2021 г. Окончательный вариант – 2 декабря 2021 г.
Received – August 03, 2021. The final version – December 2, 2021.