УДК 621.391

Д.В. Сумцов[1], Б.П. Томашевский[2], А.М. Носик[1]

[1]*Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков*
[2]*Львовский институт сухопутных войск им. гетмана Петра Сагайдачного НУ «ЛП», Львов*

ОБЩИЙ ПОКАЗАТЕЛЬ ЭФФЕКТИВНОСТИ ПЕРЕДАЧИ ДАННЫХ В КОМПЬЮТЕРНОЙ СЕТИ

Рассматриваются показатели и критерии эффективности криптографических средств защиты информации в компьютерных системах и сетях, обосновывается общий показатель эффективности обмена данными между пользователями компьютерной сети. Исследуется эффективность обмена данными в компьютерных системах и сетях на основе введенного показателя эффективности.

Ключевые слова: *компьютерные сети и системы, обобщенный показатель эффективности обмена данными.*

Введение

Увеличение объемов обрабатываемых и передаваемых данных в компьютерных системах и сетях, прежде всего в банковских системах, в системах управления крупными финансовыми и промышленными организациями, предприятиями энергетического сектора, транспорта, в системах управления и связи военного назначения требует новых подходов к протоколам и механизмам обеспечения безопасности передаваемых данных [1 – 6]. Оценку эффективности обмена данными в компьютерной сети проводят на основании частных критериев и показателей системы связи [4 – 6], что не позволяет в полной мере оценить ее эффективность. Актуальной задачей в этом смысле является обоснование общего показателя эффективности обмена данными в компьютерной сети.

Целью данной статьи является обоснование общего показателя эффективности обмена данными в компьютерной сети, исследование основных показателей сети на основе введенного показателя.

Основной материал

1. Анализ показателей и критериев эффективности криптографических средств защиты информации, обоснование общего показателя эффективности обмена данными в компьютерной сети. При рассмотрении функционирования компьютерной сети общий показатель эффективности обмена данными должен включать в себя показатель конфиденциальности и частные показатели системы связи – достоверность и оперативность.

Под *конфиденциальностью* [1, 6] (информационной скрытностью) понимается обеспечение защиты всех данных, передаваемых между любыми двумя пользователями в течение определенного времени. Наиболее общим подходом к обеспечению безопасности в точках уязвимости компьютерных сетей является использование шифрования. Таким образом, обеспечение конфиденциальности (информационной скрытности) путем реализации механизма защиты информации может оцениваться как вероятностно-временной показатель криптографической стойкости – безопасное время $T_Б$, характеризующее время безопасной работы рассматриваемого криптоалгоритма при условии применения противником различных методов криптоанализа.

По определению, безопасное время определяется по критерию минимального риска:

$$T_Б = \min\left\{T_{Б_1}, T_{Б_2}, ..., T_{Б_L}\right\}, \qquad (1)$$

где $T_{Б_i}$ – время безопасной работы рассматриваемого криптоалгоритма при условии применения противником *i*-ого метода криптоанализа; L – число известных методов криптоанализа для рассматриваемого криптоалгоритма.

В соответствии с основными положениями теории сложности время, затрачиваемое алгоритмом, как функция размера задачи, называется *временно́й сложностью* этого алгоритма [1, 6, 8]. Поведение этой сложности в пределе при увеличении размера задачи называют *асимптотической временно́й сложностью* алгоритма. Аналогично определяется *емкостная* и *асимптотическая емкостная сложность* алгоритма.

Обозначим B_i – временную сложность алгоритма, реализующего *i*-ый метод криптоанализа. Тогда соответствующий показатель безопасного времени $T_{Б_i}$ запишется в виде:

$$T_{Б_i} = \frac{B_i}{\xi \cdot \Psi}, \qquad (2)$$

где $\xi = 31622400$ – числовой коэффициент для пересчета секунд в годы; Ψ – производительность вычислительной системы, доступной криптоаналитику (противнику).

Тогда с учетом (2) выражение (1) перепишется в виде:

$$T_Б = \min\left\{\frac{B_1}{\xi\cdot\Psi}, \frac{B_2}{\xi\cdot\Psi}, ..., \frac{B_L}{\xi\cdot\Psi}\right\},$$

что эквивалентно следующей записи:

$$T_Б = \frac{B_{min}}{\xi\cdot\Psi},$$

где B_{min} – временная сложность алгоритма, реализующего наилучший известный метод криптоанализа.

Требования к безопасному времени $T_Б$ работы криптоалгоритма устанавливаются исходя из категории ценности обрабатываемой информации, ее приоритетности и принадлежности. На сегодняшний день общепринятым требованием к безопасному времени для информации любой категории ценности является условие $T_Б > 200$ лет.

Таким образом, общим требованием к безопасному времени информации является

$$T_Б \geq T_Д,$$

где $T_Д$ – допустимое безопасное время работы криптоалгоритма.

Под *достоверностью* [1, 4, 6] (информационной надежностью) передачи данных понимается степень соответствия принятых сообщений переданным. Достоверность зависит от параметров самой компьютерной сети, степени ее технического совершенства и условий работы (тип и состояние каналов связи, метеорологические показатели, вид и интенсивность помех, организационные мероприятия соблюдения правил радиообмена и эксплуатации аппаратуры). Количественно достоверность передачи может оцениваться [4]:

вероятностью ошибочного приема единичного элемента (потерей достоверности)

$$P_0 = \lim_{n_{общ}\to\infty} \frac{n_{ош}}{n_{общ}},$$

где $n_{ош}$ и $n_{общ}$ – количество ошибочно принятых и общее число переданных единичных элементов соответственно;

вероятностью ошибочного приема пакета данных

$$P_{ош\,п} = \lim_{N_{общ}\to\infty} \frac{N_{ош}}{N_{общ}},$$

где $N_{ош}$ и $N_{общ}$ – количество ошибочно принятых и общее число переданных кодовых последовательностей (пакетов) соответственно;

вероятностью правильного приема единичного элемента $P_{0\,пр}$ и вероятностью правильного приема пакета $P_{пр\,п}$, причем

$$\begin{aligned} P_{0\,пр} + P_0 &= 1; \\ P_{пр\,п} + P_{ош\,п} &= 1. \end{aligned} \qquad (3)$$

Вероятности ошибочного и правильного приема единичного элемента (P_0 и $P_{0\,пр}$) фактически являются характеристиками дискретного канала связи, вероятности $P_{ош\,п}$ и $P_{пр\,п}$ являются характеристиками компьютерной сети в целом, так как они определяются не только характером и интенсивностью помех в канале связи, видом и скоростью модуляции, но и способом защиты от ошибок в системе [1, 4].

Время доставки информации [1 – 6] – интервал времени от начала поступления сообщения данных на вход передающей части компьютерной сети до начала его выдачи получателю данных приемной частью. Время доставки $t_д$ характеризует способность компьютерной сети своевременно доставлять информацию. При передаче конфиденциальной информации кроме того во время доставки входит время шифрования отправителем пакетов данных и время расшифрования пакетов получателем соответствующим криптоалгоритмом. Анализ времени шифрования и расшифрования победителей конкурсов криптоалгоритмов AES и NESSIE [8]показывает, что для асимметричных шифров сложность реализации криптографических преобразований на 3 – 5 порядков выше, чем у аналогичных систем временной стойкости (блочно-симметричных шифров).

Таким образом, в компьютерных системах с автопереспросом (решающей обратной связью) время доставки пакета равно [4, 8]

$t_д = t_д' + \Delta t_д + t_ш + t_{расш}$ – для симметричных криптоалгоритмов,

$t_д = t_д' + \Delta t_д + (t_ш + t_{расш})^s$ – для асимметричных криптоалгоритмов,

где $t_д'$ – время доставки пакета с первой посылки; $\Delta t_д$ – время многократного повторения передачи информации при ухудшении качества канала; $t_ш$ – время шифрования пакета данных криптоалгоритмом; $t_{расш}$ – время расшифрования получателем пакета данных; s – кратность времени шифрования (расшифрования).

Время $t_д$ доставки сообщения в заданный адрес зависит от многих факторов: структуры каналов, надежности и загрузки сети, метода коммутации, наличия и характера мешающих воздействий, приводящих к ошибкам и повторным передачам. Оно является случайной величиной, характеризуемой плотностью распределения $f(t_д)$.

В каналах связи с высокой интенсивностью ошибок P_0 повышение достоверности приводит к увеличению времени доставки $t_д$ из-за увеличения числа повторных посылок пакета, и наоборот, снижение времени доставки $t_д$ за счет уменьшения числа повторных посылок пакета ведет к снижению достоверности [1, 4]. Однако большинство реальных каналов передачи данных являются нестационарными, вероятность одиночной ошибки в них изменяется во

времени в широких пределах от 10^{-9} до 10^{-2} [1, 4]. Общим требованием к достоверности информации является минимизация вероятности ошибочного приема символов сообщения $P_{ош}$ или, что эквивалентно, максимизация вероятности правильного приема $P_{пп}$. В тоже время на сегодняшний день требования к достоверности обрабатываемой и передаваемой информации существенно ужесточились и, в соответствии с руководящими документами [1, 4], допустимая вероятность ошибочного приема символов сообщения составляет:

$$P_д < 10^{-7} – 10^{-9},$$

в зависимости от категории ценности обрабатываемой информации, ее приоритетности и принадлежности.

Таким образом, общим требованием к достоверности информации является

$$P_{ош} \le P_д.$$

Поэтому для оценки эффективности функционирования компьютерной сети в качестве показателя эффективности целесообразно использовать *обобщенный показатель функциональной эффективности*. Структура построения показателя такова, что в ней объединены две основные характеристики системы: требуемая вероятность достижения цели с требуемым показателем обеспечения конфиденциальности (информационной скрытности) в определенных условиях внешней среды и при определенном уровне влияния внутренних случайных факторов; затраты, которые необходимо произвести в указанных условиях для достижения цели с требуемой вероятностью.

Показатель функциональной эффективности системы имеет вид

$$W = \frac{P}{Q},$$

где P – вероятность достижения цели операции в заданных условиях; Q – затраты, необходимые для выполнения цели операции.

В качестве вероятности достижения цели операции целесообразно использовать вероятность безошибочной доставки пакета $P_{пр\,п}$

$$P_{пр\,п} = (1 - P_0)^n,$$

где P_0 – вероятность ошибки бита в канале передачи данных; n – количество бит в пакете

Затраты, необходимые для обеспечения безошибочной доставки пакета, определяются вводимой избыточностью. Поэтому в качестве показателя вводимой избыточности может выступать *коэффициент избыточности* γ – величина, обратная полезной (эффективной) скорости передачи R, которая при фиксированной пропускной способности C измеряется числом бит информации, содержащихся в одном пакете

$$W = \frac{P_{пр\,п}}{\gamma}, \qquad (4)$$

где $\gamma = \frac{1}{R} = \frac{t_д}{h}$, (4а)

где $t_д$ – время доставки пакета; h – число информационных разрядов (бит) пакета.

Кроме того, для учета обеспечения требуемой конфиденциальности (информационной скрытности) передаваемых данных, в состав показателя эффективности необходимо ввести величину, характеризующую временную сложность (стойкость) используемого в системе шифра – количество операций, необходимое для вскрытия шифра злоумышленником B. Так как данная величина имеет достаточно высокий порядок (около $10^{19} – 10^{77}$), удобнее использовать ее десятичный логарифм. Тогда обобщенный показатель эффективности примет вид

$$W = \frac{h}{t} \cdot \lg B \cdot (1 - P_0)^n.$$

Данный показатель, включая в себя частные показатели достоверности, конфиденциальности и времени доставки данных в компьютерной сети, в сущности, отражает скорость достоверной и конфиденциальной передачи данных компьютерной сети, позволяющий оценивать эффективность сети в широком диапазоне интенсивностей ошибок в канале передачи данных, при различных скоростях передачи R.

Вероятность безошибочной доставки пакета $P_{пр\,п}$ по определению лежит в диапазоне (0, 1). Эффективная скорость R и временная сложность алгоритма, реализующего метод криптоанализа $\lg B$ в общем случае лежат в диапазоне (0, +∞). Для перехода из диапазона (0, +∞) в диапазон (0, 1) удобно воспользоваться формулой

$$x' = \frac{x - 1}{x},$$

обладающей следующими свойствами:

$$\lim_{x \to +0} \frac{x-1}{x} = -\infty, \quad \lim_{x \to 1} \frac{x-1}{x} = 0, \quad \lim_{x \to \infty} \frac{x-1}{x} = 1.$$

Заменив значения $\frac{h}{t}$ и $\lg B$ эквивалентными им, получим

$$\frac{\frac{h}{t} - 1}{\frac{h}{t}} = \frac{h - t}{h};$$

$$W = \frac{h - t}{h} \cdot \frac{\lg B - 1}{\lg B} \cdot (1 - P_0)^n.$$

Если вместо показателя временной сложности криптоалгоритма $\lg B$ использовать безопасное время работы криптоалгоритма

$$T_{Б_i} = \frac{B_i}{\Psi},$$

где Ψ – производительность вычислительной системы, доступной криптоаналитику (противнику), то

$$W = \frac{h-t}{h}\cdot\frac{t-1}{t}\cdot(1-P_0)^n = \frac{h-t}{h}\cdot\frac{\frac{B}{\Psi}-1}{\frac{B}{\Psi}}\cdot(1-P_0)^n = \frac{h-t}{h}\cdot\frac{B-\Psi}{B}\cdot(1-P_0)^n. \quad (5)$$

Так как время доставки пакета t, входящее в (5), является случайной величиной, то возможно оценить только его математическое ожидание m_t,. В этом случае выбор оптимальной стратегии функционирования компьютерной сети u* из множества допустимых стратегий U целесообразно осуществлять по критерию наибольшего среднего результата, т.е.

$$W(u^*) = \max_{u_i \in U} W(u_i), \quad (6)$$

где

$$W(u_i) = \frac{n^{(u_i)} - t^{(u_i)}}{n^{(u_i)}}\cdot\frac{B^{(u_i)} - \Psi^{(u_i)}}{B^{(u_i)}}\cdot P_{\text{пр п}}{}^{(u_i)},$$

$W(u_i)$ – показатель эффективности компьютерной сети при выбранной стратегии (методе повышения достоверности) u_i;

$n^{(ui)}$ – число информационных разрядов пакета при выбранной стратегии u_i;

$t^{(ui)}$ –время доставки пакета t при выбранной стратегии u_i;

$B^{(ui)}$ – количество операций, необходимое для вскрытия криптоалгоритма злоумышленником при выбранной стратегии u_i;

$\Psi^{(ui}$ – производительность вычислительной системы, доступной криптоаналитику (противнику) при выбранной стратегии u_i;

$P_{\text{пр п}}{}^{(ui)}$ – вероятность правильной доставки пакета при выбранной стратегии;

U – множество допустимых стратегий (методов повышения достоверности, используемых в компьютерной сети).

При этом отдельные показатели должны удовлетворять системе ограничений

$$\left\{T_Б \ge T_Д, P_{ош} \le P_Д, t_д \le t_Д\right\} \quad (7)$$

при минимизации времени доставки кадра информации.

Выбранные общий показатель и критерий эффективности компьютерной сети позволяют получить численные значения, характеризующие скорость достоверной и конфиденциальной передачи данных в компьютерной сети и произвести сравнение существующих протоколов компьютерной сети по эффективности обмена данными между двумя узлами.

Проведем исследование основных показателей достоверной и конфиденциальной доставки данных в компьютерных системах с использованием обобщенного показателя эффективности компьютерной сети.

2. Исследование эффективности обмена данными в компьютерной сети на основе общего показателя эффективности. Оценим показатель эффективности компьютерной сети (W_i) при различных стандартных длинах кадров стека протоколов X.25. Зафиксируем показатель временной сложности криптоалгоритма $B = 10^{24}$ групповых операций; производительность вычислительной системы, доступной криптоаналитику (противнику) $\Psi = 10^{15}$ групповых операций/с; длины кадров выберем для W_1 – 128 бит, для W_2 – 1024 бита, W_3 – 4096 бит, W_4 – 32768 бит. На рис. 1 представлены зависимости W_i от вероятности ошибки при использовании асимметричных алгоритмов шифрования для обеспечения конфиденциальности передачи данных, на рис. 2 зависимости при использовании симметричных алгоритмов шифрования.

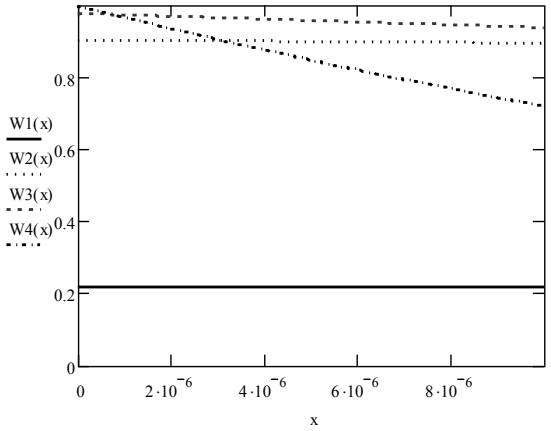

Рис. 1. Зависимость показателя эффективности компьютерной сети от вероятности ошибки при асимметричных алгоритмах шифрования

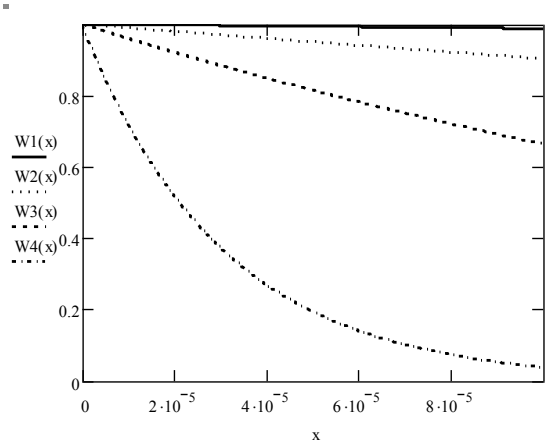

Рис. 2. Зависимость показателя эффективности компьютерной сети от вероятности ошибки при симметричных алгоритмах шифрования

Представленные на рис. 1, 2 зависимости свидетельствуют, что при увеличении стандартных длин кадров и вероятности ошибки, обобщенный показатель эффективности сети резко падает, при этом использование асимметричных схем шифрова-

ния значительно влияет на показатель эффективности сети, чем при симметричных схемах шифрования. Проведем исследования показателя эффективности компьютерной сети при различных временных стойкостях шифрования. Зафиксируем показатель временной сложности криптоалгоритма $B = 10^{24}$ групповых операций; производительность вычислительной системы, доступной криптоаналитику (противнику) $\Psi_1 = 10^{10}$ групповых операций/с; $\Psi_2 = 10^{12}$ групповых операций/с; $\Psi_3 = 10^{14}$ групповых операций/с; $\Psi_4 = 10^{15}$ групповых операций/с. На рис. 3 представлены зависимости W_i от стойкости шифрования при использовании асимметричных алгоритмов шифрования для обеспечения конфиденциальности передачи данных, на рис. 4 зависимости при использовании симметричных алгоритмов шифрования. Анализ зависимостей показывает, что эффективности компьютерной сети прямопропорциональна стойкости шифра. Проведем исследования времени доставки кадра при различных вероятностях ошибки в канале передачи.

$$W3(b) := \frac{h - t \cdot b - \Psi 3}{h \cdot b} \cdot (1 - Po)^h \qquad W4(b) := \frac{h - t \cdot b - \Psi 4}{h \cdot b} \cdot (1 - Po)^h$$

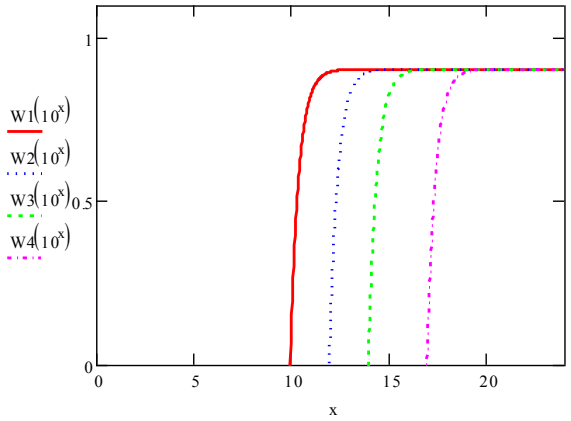

Рис. 3. Зависимость показателя эффективности компьютерной сети от стойкости шифрования при асимметричных алгоритмах шифрования

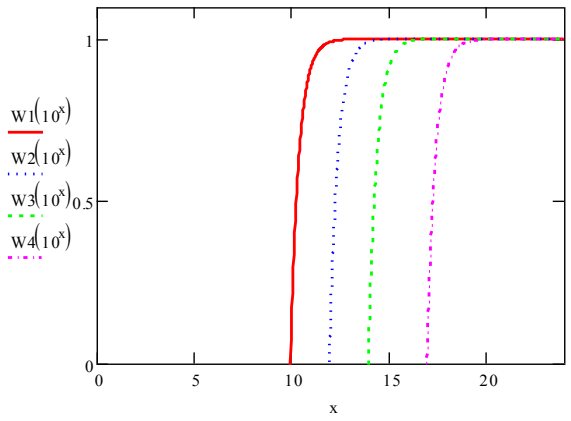

Рис. 4. Зависимость показателя эффективности компьютерной сети от стойкости шифрования при симметричных алгоритмах шифрования

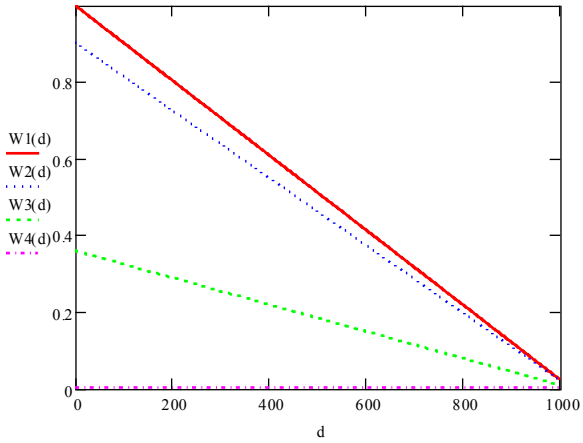

Рис. 5. Зависимость времени доставки кадра от вероятности ошибки в канале передачи при асимметричных алгоритмах шифрования

Зафиксируем показатель временной сложности криптоалгоритма $B = 10^{24}$ групповых операций; производительность вычислительной системы, доступной криптоаналитику (противнику) $\Psi_1 = 10^{15}$ групповых операций/с. Вероятность ошибки в оптоволоконных кабелях $Po_1 = 10^{-9}$; вероятность ошибки в витой паре UTP (категории 3), коаксиальном кабеле $Po_2 = 10^{-4}$; в воздушных телеграфных линиях связи $Po_3 = 10^{-3}$; в воздушных телефонных линиях связи $Po_4 = 10^{-2}$. На рис. 5 представлены зависимости времени доставки кадра от вероятности ошибки в канале передачи при использовании асимметричных алгоритмов шифрования для обеспечения конфиденциальности передачи данных, на рис. 6 зависимости при использовании симметричных алгоритмов шифрования. Анализ приведенных на рис. 5, 6 зависимостей показывает, что при использовании каналов передачи с меньшей вероятностью ошибки в канале время доставки кадра значительно сокращается.

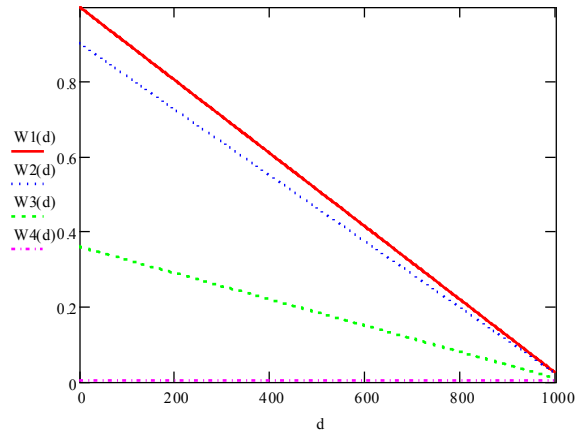

Рис. 6. Зависимость времени доставки кадра от вероятности ошибки в канале передачи при симметричных алгоритмах шифрования

Выводы

Таким образом, как показали проведенные исследования, предложенный общий показатель эффективности обмена данными в компьютерной сети позволяет всесторонне оценить протоколы обмена данными в компьютерных сетях.

Практическое использование введенного показателя позволит более точно оценивать эффективность протоколов обмена данными, используемых в компьютерных сетях.

Перспективным направлением дальнейших исследований является оценка эффективности протоколов обмена данных в реальных сетях при различных методах управления обменом информацией и используемых процедурах обеспечения конфиденциальности.

Список литературы

1. Ирвин Дж. Передача данных в сетях и инженерный подход / Дж. Ирвин, Д. Харль. – СПб.: Питер, 2002. – 405 с.

2. Олифер В.Г. Компьютерные сети / В.Г. Олифер. – СПб.: Питер, 2002. – 864 с.

3. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 1999. – 150 с.

4. Скляр Б. Цифровая связь. Теоретические основы и практическое применение: пер. с англ. / Б. Скляр. – М.: Вильямс, 2003. – 1104 с.

5. Столлингс В. Компьютерные системы передачи даннях / В. Столлингс. – М.: Вильямс, 2002. – 928 с.

6. Столлингс В. Криптография и защита сетей: принципы и практик / В. Столлингс. – 2-е изд. – М.: Вильямс, 2001. – 672 с.

7. Federal Criteria for Information Technology security. – NIST, NSA, US Government, 1993. – 216 p.

8. Cryptrec. Cryptrec liaison report to ISO/IEC 18033-2 and 18033-3 // Technical report, ryptography Research and Evaluation Committees, October 2002. – 150 p.

Поступила в редколлегию 25.03.2009.

Рецензент: д-р техн. наук, проф. А.А. Кузнецов, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ЗАГАЛЬНИЙ ПОКАЗНИК ЕФЕКТИВНОСТІ ПЕРЕДАЧІ ДАНИХ У КОМП'ЮТЕРНІЙ МЕРЕЖІ

Д.В. Сумцов, Б.П. Томашевський

Розглядаються показники й критерії ефективності криптографічних засобів захисту інформації в комп'ютерних системах і мережах, обґрунтовується загальний показник ефективності обміну даними між користувачами комп'ютерної мережі. Досліджується ефективність обміну даними в комп'ютерних системах і мережах на основі уведеного показника ефективності.

Ключові слова: *комп'ютерні мережі та системи, узагальнений показник ефективності обміну даними.*

THE GENERAL FACTOR TO EFFICIENCY DATA COMMUNICATION IN COMPUTER NETWORK

D.V. Sumcov, B.P. Tomashevskiy

They are considered factors and criteria to efficiency of the cryptographic meanses of protection information in computer system and set, is motivated general factor to efficiency of the exchange given between user of the computer network. Efficiency of the exchange given is researched in computer system and set on base of the entered factor to efficiency.

Keywords*: computer networks and systems, generalised factor to efficiency of the exchange data.*