УДК 681.3

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ ВЫЯВЛЕНИЯ СКРЫТЫХ КАНАЛОВ

Королёв Игорь Дмитриевич
доктор технических наук, доцент

Савчук Дмитрий Владимирович
кандидат технических наук

Мызников Олег Николаевич
кандидат технических наук, доцент

Сызранов Алексей Павлович
кандидат технических наук

Логвиненко Светлана Викторовна

Краснодарское высшее военное училище (военный институт) имени генерала армии С.М. Штеменко, Краснодар, Россия

В данной статье представлена математическая модель системы выявления скрытых каналов в сетях пакетной передачи данных автоматизированных систем, разработанная на основе анализа принципов построения и модуляции сигналов, передаваемых по скрытым каналам

Ключевые слова: СКРЫТЫЙ КАНАЛ, МАТЕМАТИЧЕСКАЯ МОДЕЛЬ, АВТОМАТИЗИРОВАННАЯ СИСТЕМА, СИСТЕМА ЗАЩИТЫ, СЕТЕВОЙ ПОТОК

UDC 681.3

MATHEMATICAL SYSTEM MODEL FOR DISCOVERY OF HIDDEN CHANNEL

Korolyov Igor Dmitrievich
Dr.Sci.Tech., assistant professor

Savchuk Dmitriy Vladimirovich
Cand.Tech.Sci.

Myznikov Olrg Nikolaevich
Cand.Tech.Sci., assistant professor

Syzranov Aleksey Petrovich
Cand.Tech.Sci.

Logvinenko Svetlana Viktorovna

Shtemenko High Military School (Military Institute), Krasnodar, Russia

In the given article, the mathematical system model for discovery of hidden channels in the network of packet data communication automatic systems, designed on the base of the analysis of building principles and inflexions of signals, sent through hidden channels is presented

Keywords: HIDDEN CHANNEL, MATHEMATICAL MODEL, AUTOMATIC SYSTEM, PROTECTION SYSTEM, NETWORK FLOW

При разработке математической модели системы выявления скрытых каналов в сетях пакетной передачи данных автоматизированных систем (АС), в качестве исходных, учтены следующие условия:

1. Рассматриваемые виды скрытых каналов: детерминированный и стохастический в сетях пакетной передачи данных автоматизированных систем.

2. Параметрами модуляции являются наследуемые информативные параметры – адреса отправителей и (или) получателей в заголовках IP-дейтаграмм.

3. Свойства сетевого потока допускают возможность изменения порядка следования пакетов (протокол сетевого уровня модели TCP/IP является мутным).

4. Закладочные устройства (ЗУ) противника являются обучаемыми и обеспечивают как прием, так и передачу данных.

Данные условия были установлены в результате анализа принципов построения и модуляции сигналов, передаваемых по скрытым каналам в сетях пакетной передачи данных АС.

Согласно Ронжину [2], свойства скрытого канала возможно представить парой функций j и y. Функция j относится к узлу, реализующему скрытую передачу данных (ЗУ), и осуществляет отображение множества свойств сетевого потока S во множество $j(S)$. Функция y относится к системе защиты – $y(j(S))$, y_r – ЗУ-приемник (рис. 1).

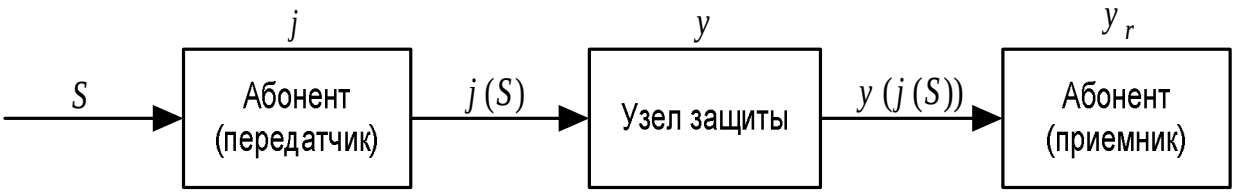

Рисунок 1 – Известное представление свойств скрытого канала отображениями конечных множеств

Так, существуют прозрачные и мутные протоколы, свойства которых определяются следующими соотношениями [2]:

прозрачный протокол: $|j(S)| = |y(j(S))|$; мутный протокол: $|j(S)| > |y(j(S))|$ (1)

Если протокол (j, y) является мутным для него верно неравенство $|j(S)| > |y(j(S))|$ – параметры модуляции сетевого потока различны и могут быть использованы для модуляции сигналов, передаваемых по СК.

Если протокол (j, y) является прозрачным, тогда верно равенство $|j(S)| = |y(j(S))|$ – параметры модуляции сетевого потока одинаковы и не могут быть использованы для модуляции сигналов, передаваемых по СК.

Применение мутного протокола может привести к нарушению безопасности информации, обрабатываемой в системе. Примерами таких нарушений являются организация скрытых каналов и махинации в системах нотариального заверения цифровых подписей [4, 5]. Так как в настоящее время отсутствуют соответствующие эффективные методы и средства выявления скрытых каналов, то функция y не учитывает наличие перестановок IP-дейтаграмм. Следовательно, каждый сигнал, передаваемый по скрытому каналу, воспринимается узлом защиты без учета порядка следования элементов.

В результате анализа принципов взаимодействия ЗУ на основе информационного протокола (j, y) определены условия приведения фрагмента сетевого потока к прозрачному виду, при сохранении мутности его элементов, обеспечивающие возможность обнаружения СК в узлах АС при защищенном взаимодействии [3]. Данные условия реализуются на основе применения протокола (a, x), где a – функция преобразования фрагмента сетевого потока, обеспечивающая приведение его к прозрачному виду, x – функция контроля преобразования a.

Возможны следующие состояния сетевого потока C до узла защиты АС: S и $j(S)$, отражающие отсутствие (рис. 2) и наличие модуляции сигнала j (рис. 3), соответственно, до узла защиты, в условиях применения протокола (a, x):

1. $j = 0$ в сетевом потоке S, в узле защиты неизвестно $j = 0$ или $j \neq 0$, тогда:

отсутствие модуляции j сигнала СК в узле защиты:

$$|a(S)| = |x(a(S))| \quad (2)$$

нарушение прозрачности протокола – наличие модуляции j *сигнала СК в УЗ, так как* $|a(S)| < |j(a(S))|$:

$$|a(S)| < |x(j(a(S)))| \quad (3)$$

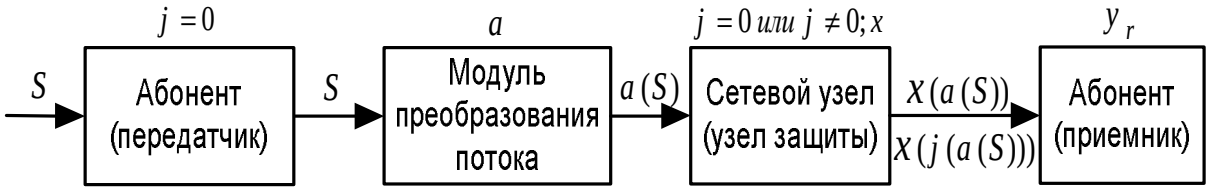

Рисунок 2 – Представление протоколов преобразования сетевого потока и анализа СК при отсутствии модуляции потока пакетов до узла защиты

Таким образом, соблюдение равенства (2) $|a(S)| = |x(a(S))|$ свидетельствует об отсутствии модуляции в контролируемом узле, но в отличие от (1) $|y(S)| = |y(j(S))|$, когда узел защиты, реализующий y не способен отличить сетевой поток, обладающий набором свойств $j(S)$, от сетевого потока – S, функция x наделена возможностью контроля $a(S)$.

Если $a(S)$ в процессе прохождения через узел защиты подвергнется модуляции СК j, то на выходе примет вид $j(a(S))$ и изменения будут выявлены с помощью функции контроля прозрачности x, таким образом, факт нарушения прозрачности фрагмента сетевого потока отражает неравенство (3).

2. Если в сетевом потоке S, до узла защиты, модуляция $j \neq 0$ и поток будет $j(S)$, при этом неизвестно $j = 0$ или $j \neq 0$ в узле защиты, тогда:

при отсутствии модуляции сигнала СК в узле защиты ($j = 0$*):*

$|a(j(S))| = |x(a(j(S)))|$ – очевидно, что при отсутствии модуляции сигнала в узле защиты, прозрачность не будет нарушена, но сигнал СК

будет искажен функцией a, тогда приемник y_r (ЗУ) примет сигнал $a(j(S))$ вместо $j(S)$. В таком случае для выявления сигнала, передаваемого по скрытому каналу потребуется дополнительный анализ сетевого потока.

при наличии модуляции сигнала СК в узле защиты ($j \neq 0$)*:*

$|a(j(S))| < |x(j(a(j(S))))|$ – нарушение прозрачности фрагмента сетевого потока.

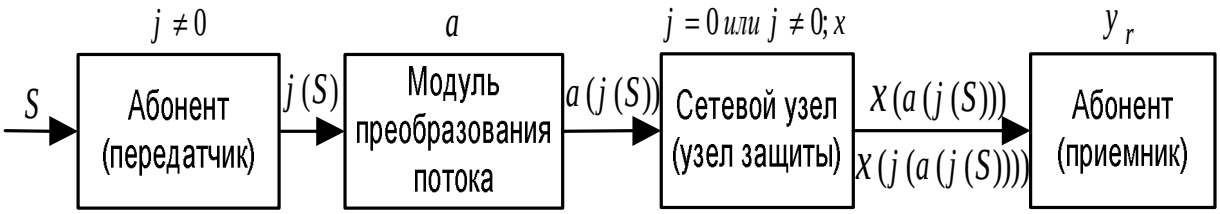

Рисунок 3 – Представление протоколов преобразования сетевого потока и анализа СК при наличии модуляции потока пакетов до узла защиты

Система выявления скрытых каналов в первоначальном состоянии не располагает информацией о наличии, либо отсутствии скрытой передачи, поэтому на участке до узла защиты сетевой поток описывается соотношениями $j(S) = C$ и $S = C$ (рис. 4).

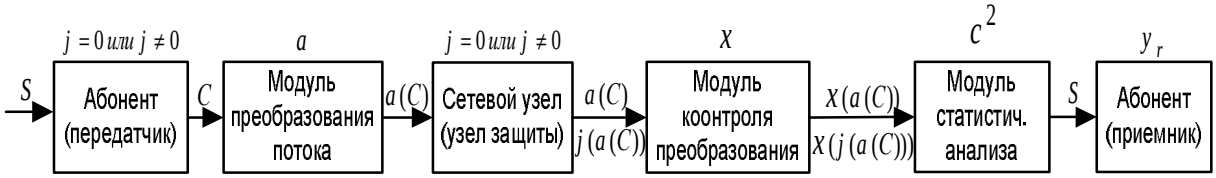

Рисунок 4 – Представление протоколов преобразования сетевого потока и анализа СК при наличии (отсутствии) модуляции потока пакетов до узла защиты

Выявление сигнала СК, сформированного в узле защиты, будет обеспечено с помощью функции контроля прозрачности x. О наличии модуляции сигнала в узле защиты свидетельствует нарушение прозрачности протокола неравенство (3).

Таким образом, определены новые условия прозрачности и мутности фрагмента сетевого потока, приведенного к прозрачному виду при сохранении мутности его элементов, представлены соотношениями (4) и (5):

$$|a(C)| = |x(a(C))| \quad (4)$$

$$|a(C)| < |x(j(a(C)))| \quad (5)$$

Но факт наличия, либо отсутствия модуляции в потоке вида C не установлен, т.е. возможно: $C = j(S)$ или $C = S$. В таком случае модуляция сигнала, передаваемого по СК, в C может быть выявлена на основе сравнения статистических характеристик C и $a(C)$.

Фрагменты сетевого потока C и $a(C)$ могут быть представлены в виде выборок:

$C = X$ – долговременная выборка и $a(C) = Y$ – текущая выборка:

$$X = (X_1, X_2, \ldots, X_{n_1}) \quad (6)$$

$$Y = (Y_1, Y_2, \ldots, Y_{n_2}) \quad (7)$$

где n_1 и n_2 – объемы выборок.

Выполнить проверку гипотезы однородности выборок возможно на основе применения статистических критериев.

Данная математическая модель отражает свойства сетевого потока при применении функций преобразования потока a и контроля изменений x, что обеспечивает возможность выявления модуляции сигналов скрытых каналов в сетевых узлах АС, а также сигнала, передаваемого по СК в сетевом потоке – на основе статистических методов. Но в результате анализа [1, 2, 3] установлена необходимость определения характеристик и контроля состояний и «реакций» системы.

Так согласно [1] если на вход системы S подается случайный процесс $X(t)$ – «входной сигнал» или «входное воздействие», система S осуществляет преобразование входного сигнала $X(t)$, в результате чего на

выходе системы S получается случайный процесс $Y(t)$, называемый «реакцией системы» S (или «выходным сигналом» системы S).

Символически преобразование случайного процесса $X(t)$, поступающего на вход системы S, в выходной сигнал $Y(t)$ можно представить в виде

$$Y(t) = A_t\{X(t)\}, \quad (8)$$

где A_t - оператор системы S.

Индекс t означает, что этот оператор осуществляет преобразование случайного процесса по аргументу t, обычно имеющему смысл времени.

Если известны любые два элемента в соотношении (8), тогда возможно вычислить третий [1]. То есть, зная характеристики входного воздействия $X(t)$ и оператор A_t, можно определить характеристики реакции системы $Y(t)$. А зная характеристики входного воздействия $X(t)$ и требования к характеристикам реакции системы $Y(t)$, можно определить оператор системы A_t.

Таким образом, предложенная математическая модель отражает свойства сетевого потока, обеспечивает возможность определения характеристик, состояний и «реакций» контролируемой системы для выявления модуляции сигналов скрытых каналов в сетевых узлах АС, а также, передаваемых по СК в сетевом потоке.

Литература

1. Вентцель, Е. С. Теория случайных процессов и ее инженерные приложения / Е. С. Вентцель, Л. А. Овчаров. – М. : Высшая школа, 2000. – 383 с.

2. Ронжин, А. Ф. Расширения информационных протоколов, основанных на отображениях конечных множеств [Текст] / А. Ф. Ронжин // Дискретная математика. – 2004. – Т. 16. – Вып. 2. – С. 11 – 16.

3. Сызранов, А. П. Метод выявления скрытых каналов на основе контроля фрагмента сетевого потока, приведенного к прозрачному виду / Сызранов А. П. // Естественные и технические науки. – М.: Спутник +, 2009.

4. Lampson, B. W. A Note of the Confinement Problem/ B. W. Lampson // Communications of ACM. – 1973. – V. 10:16. – P. 613 – 615.

5. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. – New York: John Wiley & Sons, 2nd edition, 1996.