УДК 681.3

РАЗРАБОТКА МЕТОДОВ ПРОТИВОДЕЙСТВИЯ ИСПОЛЬЗОВАНИЮ СКРЫТЫХ КАНАЛОВ В СЕТЯХ С ПАКЕТНОЙ ПЕРЕДАЧЕЙ ДАННЫХ

Назаров Игорь Владимирович
кандидат технических наук

Сызранов Алексей Павлович
кандидат технических наук

Зимонин Дмитрий Викторович
кандидат технических наук

Козленко Сергей Леонидович

Филиал Военной академии связи (г. Краснодар), Краснодар, Россия

Мызников Олег Николаевич
кандидат технических наук, доцент

Кубанский государственный технологический университет, Краснодар, Россия

В данной статье представлена модель, с помощью, которой возможно определить основные свойства скрытых каналов в сетях с пакетной передачей данных, а также методы противодействия скрытым каналам, разработанные на основе предложенной модели

Ключевые слова: МОДЕЛЬ, СКРЫТЫЙ КАНАЛ, СЕТЕВОЙ ПРОТОКОЛ, СЕТЕВАЯ АТАКА

UDC 681.3

DEVELOPING A COUNTERMEASURES TO USING COVERT CHANNELS IN PACKET-SWITCHED NETWORKS

Nazarov Igor Vladimirovich
Cand.Tech.Sci.

Syzranov Alexey Pavlovich
Cand.Tech.Sci.

Zimonin Dmitriy Victorovich
Cand.Tech.Sci.

Kozlenko Sergey Leonidovich

The Branch of Military Academy of Communications, Krasnodar, Russia

Myznikov Oleg Nikolaevich
Cand.Tech.Sci., associate professor

Kuban State Technological University, Krasnodar, Russia

In the given article a model which allows defining general characteristics of covert channels in packet-switched networks as well as countermeasures to covert channels developed on the basis of the model in question are presented

Keywords: MODEL, COVERT CHANNEL, NETWORKING PROTOCOL, DENIAL-OF-SERVICE ATTACK

Высокая эффективность современных средств защиты информации подтверждается опытом их практического применения, но существуют способы нарушения безопасности информации, основанные на использовании скрытых каналов (СК). Под скрытым каналом, согласно [1], понимается непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности (ПБ).

Технологии виртуальных частных сетей (VPN, Virtual Private Network) позволяют обеспечить высокий уровень конфиденциальности ин-

формации, передаваемой через информационно-вычислительные сети общего пользования (ИВС ОП). Взаимодействие узлов автоматизированной системы (АС) через каналы ИВС ОП с применением технологии VPN обеспечивается установкой пограничных узлов защиты (УЗ), состоящих из шифровального средства (ШС) и межсетевого экрана (МЭ) (рис. 1).

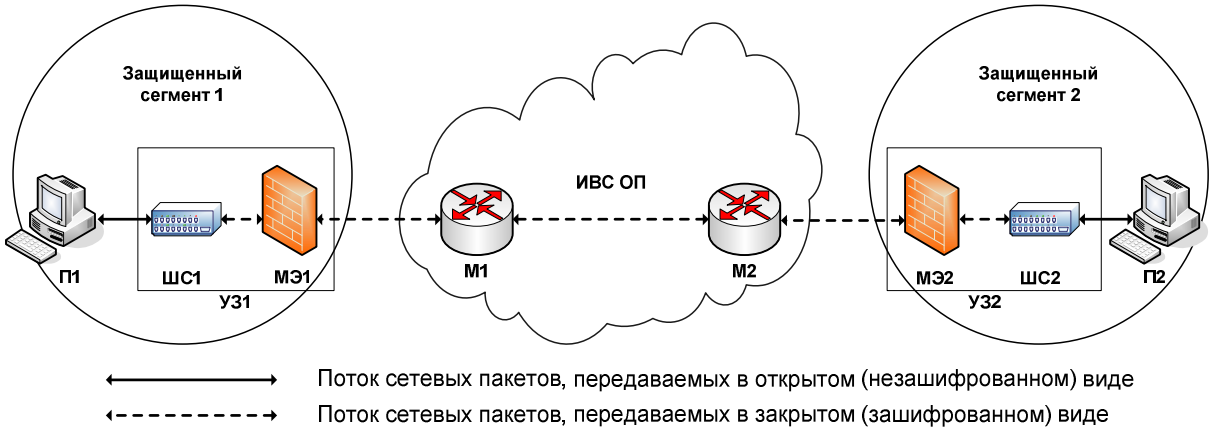

Рисунок 1 – Схема взаимодействия узлов АС через каналы ИВС ОП с применением технологии VPN

Скрытые каналы, нарушая системную (сетевую) политику безопасности, в большинстве случаев остаются необнаруженными современными системами защиты информации (СЗИ), поэтому применение СЗИ является неэффективным, а злоумышленник получает возможность преодолеть элементы защиты и осуществить несанкционированное воздействие (НСВ) на защищаемые ресурсы с нарушением установленных прав и/или правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к уничтожению или сбою функционирования носителя информации.

В настоящее время разработаны различные методы выявления и нейтрализации скрытых каналов как в хост-системах, так и в сетях пакетной передачи данных. Традиционный метод выявления скрытых каналов, представленный в работах [2, 3], опирается на модель зависимости. С методом зависимостей непосредственно связан метод поиска скрытых кана-

лов на основе матрицы разделяемых ресурсов, рассмотренный в работе [4], где предполагается, что система полностью описывается переменными *a, b, … z*. Такая матрица показывает потенциальные информационные потоки между переменными. Метод, описанный в работе [5], обеспечивает достаточно низкий уровень ложных тревог, но для его реализации могут потребоваться значительные вычислительные ресурсы.

В результате анализа известных методов борьбы со СК установлено, что данные методы ориентированы на отдельные типы СК, при этом не учитываются многие параметры, необходимые для обнаружения скрытой передачи в информационно-вычислительных системах, поэтому в настоящее время не разработаны и не внедрены эффективные средства (системы) выявления и нейтрализации скрытых каналов.

Пусть φ – функция несанкционированного воздействия на сетевой поток, обладающий ограниченным набором свойств *S*. Данная функция выполняется закладочным устройством ЗУ1, внедренным в маршрутизатор М2 (рис. 1).

Пусть ψ – функция обеспечения безопасности информации, выполняемая каждым узлом защиты по отношению к сетевому потоку, обладающему ограниченным набором свойств *S*. Данная функция выполняется узлами защиты УЗ1 и УЗ2.

Тогда, согласно [6] сетевой поток, поступающий на УЗ2 обладает набором свойств $\varphi(S)$, вместо «ожидаемого» на данном участке набора свойств *S*. Следовательно, УЗ2 применяет по отношению к входящему потоку функцию $\psi(\varphi(S))$ вместо $\psi(S)$.

Предположим, что если $\psi(\varphi(S))=\psi(S)$, сетевой поток проходит через УЗ2, не нарушая существующих правил разграничения доступа, и поступает на узел П2.

Пусть ψ_r – функция несанкционированного анализа сетевого потока.

Функция ψ_r выполняется ЗУ2, внедренным в П2. Данная функция возвращает успешный результат при $\psi_r = \left(\varphi(S)\right)$ и неудачный результат при $\psi_r(S)$.

Модель СК в сетях пакетной передачи данных построена с учетом всех этапов скрытой передачи между закладочными устройствами (рис. 2).

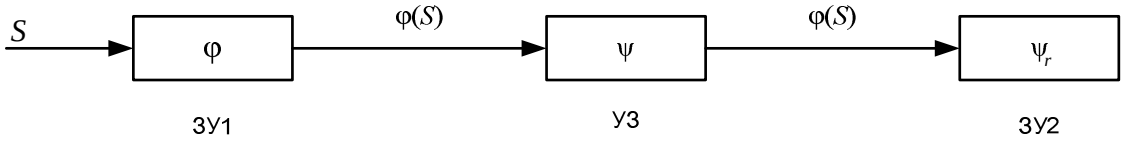

Рисунок 2 – Модель СК в сетях пакетной передачи данных

Рассмотрим сетевую атаку на автоматизированную систему при использовании СК с модуляцией потока пакетов по признаку длин применительно к представленной модели.

В отношении свойств *S* сетевого потока в [7] установлены следующие допущения:

- сетевой поток содержит только IP-дейтаграммы с длинами четырех различающихся видов – *a*, *b*, *c*, *d*;
- в сетевом потоке не могут подряд следовать две и более IP-дейтаграмм с длинами одного вида.

Исходя из указанных допущений, все IP-дейтаграммы сетевого потока можно условно разделить на группы по 4 пакета с различающимися длинами. Каждая группа содержит определенную комбинацию длин IP-дейтаграмм. Количество возможных комбинаций определяет состав множества *S*.

Таким образом, множество *S* состоит из перестановок длины 4, каждая из которых содержит элементы *a*, *b*, *c*, *d*. При этом $|S| = 4! = 24$.

Перестановка *abcd* является строго возрастающей последовательностью длин сетевых пакетов. Элементы множества *S* могут быть использованы для модуляции сигналов «0» и «1».

Пусть, для модуляции сигнала «0» будут использоваться перестановки *acdb*, *bdca*, *adcb*, *bcda*, а для модуляции сигнала «1» – перестановки *cabd*, *dbac*, *dabc*, *cbad*, способы модуляции подробно представлены в [7].

Пусть $\varepsilon_1(S)$ – множество всех перестановок, которые могут быть использованы для модуляции сигнала «0», и $\varepsilon_2(S)$ – множество всех перестановок, которые могут быть использованы для модуляции сигнала «1».

Тогда,

$$\varepsilon_1(S)=\{acdb, bdca, adcb, bcda\}, \qquad \varepsilon_2(S)=\{cabd, dbac, dabc, cbad\}.$$

Таким образом, в данном примере, $|\varphi(S)|=8$, $|\varepsilon_1(S)|=|\varepsilon_2(S)|=4$.

Пусть функция ψ, выполняемая УЗ2, не учитывает порядок следования пакетов. Тогда будем считать, что каждый элемент $s\in S$ интерпретируется УЗ2 как сочетание *abcd*, в котором порядок следования элементов не имеет значения, $\psi(S)=\psi(\varphi(S))=\{abcd\}$, $|\psi(S)|=|\psi(\varphi(S))|=1$.

Равенство $\psi(S)=\psi(\varphi(S))$ обозначает, что УЗ2 не способен отличить сетевой поток, обладающий набором свойств *S*, от сетевого потока, обладающего набором свойств $\varphi(S)$.

Если результатом отображения ψ для любой перестановки $s\in S$ является сочетание *abcd*, то перестановка без изменений передается в защищенный сегмент 2, где поступает на узел П2, в который внедрено ЗУ2.

ЗУ2 осуществляет несанкционированный анализ сетевого потока, применяя функцию ψ_r, с помощью которой определяет состав множеств $\varepsilon_1(S)$ и $\varepsilon_2(S)$. Таким образом, ЗУ2 переходит в состояние готовности приема от ЗУ1 определенной команды для выполнения несанкционированного воздействия на ресурсы АС.

В [6] определено, что пара отображений (φ,ψ), где $\varphi,\psi \in C(S)$ и $C(S)$ – множество всех отображений множества S в себя, называется информационным протоколом на S. Протокол (φ,ψ) называется прозрачным, если $|\varphi(S)| = |\psi(\varphi(S))|$, и мутным, если $|\varphi(S)| > |\psi(\varphi(S))|$.

Применительно к модели СК, функции φ и ψ представляют информационный протокол (φ,ψ), как определенные правила, которые описывают функции обеспечения безопасности информации ψ по отношению к сетевому потоку, обладающему свойствами $\varphi(S)$, и содержащему сигнал, передаваемый с применением СК.

Прозрачный протокол – это протокол (φ,ψ), свойства которого недостаточны для организации передачи сигналов с применением СК, т.е. если $|S| = 1$, то $|\varphi(S)| = 1$, следовательно, $|\varphi(S)| = |\psi(\varphi(S))|$.

Мутный протокол – это протокол (φ,ψ), свойства которого достаточны для организации передачи сигналов с применением СК, т.е. если $|S| \geq 2$, то $|\varphi(S)| \geq 2$, следовательно, $|\varphi(S)| > |\psi(\varphi(S))|$.

Анализ представленной модели СК в сетях с пакетной передачей данных АС показал, что условиями существования СК являются:

- отсутствие в составе средств обеспечения безопасности информации АС функции, способной выявить отличие между S и $\varphi(S)$;
- наличие в сетевом потоке свойств, с применением которых возможно осуществлять модуляцию $\varphi(S)$ сигналов «0» и «1».

Следовательно, для обеспечения противодействия СК, необходимо исключить возможность выполнения одного из перечисленных условий.

Для включения в состав средств обеспечения безопасности информации АС функции, способной выявить отличие между S и $\varphi(S)$, необходимо обеспечить непрерывный анализ свойств S сетевого потока, в реальном времени, с применением статистических или других методов.

Наличие в сетевом потоке свойств, с применением которых возможно осуществлять модуляцию $\varphi(S)$ сигналов «0» и «1», в большинстве случаев (для большинства признаков модуляции), является неотъемлемой составляющей сетевого протокола, необходимой для обеспечения межсетевого взаимодействия. Следовательно, для организации противодействия необходимо решение, препятствующее применению нарушителем свойств сетевого потока *S*, для осуществления скрытой передачи сигналов по СК. При этом, для обеспечения межсетевого взаимодействия в соответствии с установленным протоколом, необходимые свойства *S* сетевого потока должны оставаться неизменными, даже если они могут быть применены злоумышленником для организации скрытой передачи сигналов по СК.

Для реализации метода приведения мутного протокола к прозрачному протоколу при изменении количества свойств сетевого потока необходимо и достаточно включить в состав средств обеспечения безопасности информации функцию δ_x [7], обеспечивающую изменение свойств *S* сетевого потока таким образом, что

$$|\delta_x(S)| = |\delta_x(\varphi(S))| = Z, \qquad Z \cap S = \varnothing.$$

Применительно к приведенному выше примеру СК с модуляцией сетевого потока по признаку длин IP-дейтаграмм, использование функции δ_x обеспечит выравнивание их длин таким образом, что

$$\delta_x(S) = \delta_x(\varphi(S)) = Z = \{d\}.$$

Поскольку УЗ2 проверяет пакеты входящего сетевого потока на предмет соответствия правилу ψ, и данное правило не учитывает порядок следования пакетов, то

$$\psi(\delta_x(S)) = \psi(\delta_x(\varphi(S))) = \psi(Z) = \{d\}.$$

Тогда,

$$|\delta_x(\varphi(S))| < |\varphi(S)| \le |S|,$$

$$|\delta_x(\varphi(S))| = |\psi(\delta_x(\varphi(S)))| = |\psi(\varphi(S))|,$$

следовательно, протокол (φ,ψ) прозрачен и передача сигналов «0» и «1» с применением модуляции пакетов по признаку длины невозможна.

Таким образом, представлен метод противодействия СК в сетях пакетной передачи данных АС, основанный на применении прозрачного протокола (φ,ψ), с изменением количества свойств *S* сетевого потока.

Данный метод целесообразно применять в условиях невозможности реализации метода приведения элементов сетевого потока к прозрачному виду на этапе его формирования (до передачи в сеть). Метод приведения элементов сетевого потока к прозрачному виду не требует значительных затрат ресурсов автоматизированных систем и времени, так как исключает дополнительные преобразования сформированного сетевого потока.

Кроме того, прозрачность протокола (φ,ψ) следует рассматривать относительно применяемого признака модуляции. Например, протокол (φ,ψ) может являться прозрачным относительно признака модуляции по длинам сетевых пакетов, но при этом являться мутным относительно признака модуляции по адресам в заголовках сетевых пакетов.

В [7] представлен разработанный метод приведения мутного протокола к прозрачному протоколу без изменения количества свойств сетевого потока. Где для приведения мутного протокола к прозрачному без изменения количества свойств сетевого потока необходимо и достаточно включить в состав средств обеспечения безопасности информации функцию δ_y, обеспечивающую изменение свойств *S* сетевого потока таким образом, что

$$\left|\delta_y(S)\right| = \left|\delta_y(\varphi(S))\right| = 1.$$

Применительно к приведенному выше примеру СК с модуляцией сетевого потока по признаку длин IP-дейтаграмм, применение функции δ_y обеспечит равномерное распределение длин внутри каждой группы из четырех IP-дейтаграмм так, что $\delta_y(S) = \delta_y(\varphi(S)) = \{abcd\}$.

Поскольку УЗ2 (рис. 1) проверяет пакеты входящего сетевого потока на предмет соответствия правилу ψ, и данное правило не учитывает порядок следования сетевых пакетов, то

$$\psi(\delta_y(S)) = \psi(\delta_y(\varphi(S))) = \{abcd\}.$$

Тогда,

$$\left|\delta_y(\varphi(S))\right| < \left|\varphi(S)\right| \le \left|S\right|,$$

$$\left|\delta_y(\varphi(S))\right| = \left|\psi(\delta_y(\varphi(S)))\right| = \left|\psi(\varphi(S))\right|,$$

следовательно, протокол (φ,ψ) прозрачен и передача сигналов «0» и «1» с применением модуляции пакетов по признаку длины невозможна.

Рассмотренный метод скрытой передачи является частным случаем реализации детерминированного СК на основе группировки IP-дейтаграмм.

Так как, кодирование сигналов, передаваемых по СК может осуществляться не только на основе троек или четверок IP-дейтаграмм (детерминированный СК), но и на основе группирования *n* IP-дейтаграмм, либо на основе стохастического канала, где «расстояния» между информативными элементами СК, участвующими в модуляции сигнала, могут значительно отличаться от «троек», «четверок» и т.п., либо четного или нечетного количества незначимых элементов, с использованием более сложной функции φ для несанкционированного воздействия на сетевой поток. Поэтому для повышения эффективности противодействия СК возникла необходимость разработки новых методов.

Если при некоторых условиях функция δ_y не обеспечивает равномерное распределение длин внутри каждой группы из *n* IP-дейтаграмм, в частности, когда диапазон применения δ_y меньше, либо не учитывает размер или другие характеристики сигналов, передаваемых по скрытым каналам. Тогда необходимо осуществить анализ скрытых каналов и определить основные характеристики сигналов СК, которые будут учитываться при

реализации функции анализа сетевого потока ψ_a (аналогичной – ψ_r), и станут основой для эффективного противодействия с использованием δ_y.

Исходя из этого, разработан метод контроля прозрачности фрагмента сетевого потока при сохранении мутности его элементов [8]. Где в результате анализа принципов взаимодействия ЗУ на основе информационного протокола (φ,ψ) определены условия приведения фрагмента сетевого потока к прозрачному виду, при сохранении мутности его элементов, обеспечивающие возможность обнаружения СК в узлах АС при защищенном взаимодействии. Данные условия реализуются на основе применения разработанного протокола (α,ξ), где α – функция преобразования фрагмента сетевого потока, обеспечивающая приведение его к прозрачному виду, ξ – функция контроля преобразования α.

Таким образом, соблюдение равенства $|\alpha(S)|=|\xi(\alpha(S))|$ свидетельствует об отсутствии модуляции в контролируемом узле, но в отличие от $|\psi(S)|=|\psi(\varphi(S))|$, когда узел защиты, реализующий ψ не способен отличить сетевой поток, обладающий набором свойств $\varphi(S)$, от сетевого потока – S, функция ξ наделена возможностью контроля $\alpha(S)$.

Если $\alpha(S)$ в процессе прохождения через узел защиты подвергнется модуляции СК φ, то на выходе примет вид $\varphi(\alpha(S))$ и изменения будут выявлены с помощью функции контроля прозрачности ξ.

Таким образом, факт нарушения прозрачности фрагмента сетевого потока отражает неравенство $\left|\alpha(S)\right|<\left|\xi(\varphi(\alpha(S)))\right|$.

Для применения мутного протокола с восстановлением первоначальных свойств *S* сетевого потока необходимо и достаточно включить в состав средств защиты информации функцию δ_z [7], обеспечивающую изменение свойств *S* сетевого потока таким образом, что

$$\delta_z(S)=\delta_z(\varphi(S))=\varphi^{-1}(S)=S.$$

Применительно к приведенному выше примеру СК с модуляцией потока по признаку длины, применение функции δ_z обеспечит восстановление порядка следования сетевых пакетов, что является восстановлением свойств *S* сетевого потока, которые были изменены в результате преобразования $\varphi(S)$.

Поскольку узел защиты УЗ2 проверяет IP-дейтаграммы входящего сетевого потока на предмет соответствия ψ, и не учитывает порядок следования сетевых пакетов, то

$$|\psi(\delta_z(S))| = |\psi(\delta_z(\varphi(S)))| = |\psi(S)| = |\psi(\varphi(S))| = 1.$$

Протокол (φ,ψ) является мутным, поскольку

$$|\delta_z(\varphi(S))| = |\delta_z(S)| = |S| \geq |\varphi(S)| > |\psi(\varphi(S))|$$

ЗУ2 реализует функцию ψ_r, при этом успешное принятие решения возможно только при $\psi_r(\varphi(S))$, следовательно, передача сигналов «0» и «1» с применением модуляции пакетов по признаку длины невозможна, поскольку

$$\psi_r(\delta_z(\varphi(S))) = \psi_r(S).$$

Таким образом, разработанные методы являются основой методики противодействия СК, которая может быть использована при разработке перспективных систем выявления и нейтрализации скрытых каналов в сетях с пакетной передачей данных автоматизированных систем.

Список литературы:

1. ГОСТ Р 53113-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Общие положения. – М.: Стандарты, 2008. – Ч. 1.

2. Тимонина, Е. Е. Скрытые каналы (обзор) // JetInfo, 2002. – 11(114) – С. 3 – 11.

3. Handbook for the Computer Security Certification of Trusted Systems // NRL Technical Memorandum 5540:062A, 12 Feb. 1996.

4. Kemmerer, R. A. Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels //ACM Transactions on Computer Systems, 1:3, pp. 256_277, August 1983.

5. Тумоян, Е. П. Сетевое обнаружение пассивных скрытых каналов передачи данных в протоколе TCP IP / Е. П. Тумоян, М. В. Аникеев // Журнал «Информационное противодействие угрозам терроризма» – 2005. – Вып. 5.

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

7. Назаров, И. В. Разработка модели нетрадиционного информационного канала и методов противодействия нетрадиционным информационным каналам в сетях пакетной передачи данных / Назаров И.В. // Электронный журнал «Труды Кубанского Государственного Аграрного Университета». - Краснодар: КубГАУ, 2006.

8. Королев, И. Д. Математическая модель системы выявления скрытых каналов / Королев, И. Д., Савчук Д.В., Сызранов А. П., Логвиненко С.В., Мызников О.Н. // Электронный журнал «Труды Кубанского Государственного Аграрного Университета». - Краснодар: КубГАУ, 2010, № 60 (06).

References

1. GOST R 53113-2008 Informacionnaja tehnologija. Zashhita informacionnyh tehnologij i avtomatizirovannyh sistem ot ugroz informacionnoj bezopasnosti, re-alizuemyh s ispol'zovaniem skrytyh kanalov. Obshhie polozhenija. – M.: Standarty, 2008. – Ch. 1.

2. Timonina, E. E. Skrytye kanaly (obzor) // JetInfo, 2002. – 11(114) – S. 3 – 11.

3. Handbook for the Computer Security Certification of Trusted Systems // NRL Technical Memorandum 5540:062A, 12 Feb. 1996.

4. Kemmerer, R. A. Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels //ACM Transactions on Computer Systems, 1:3, pp. 256_277, August 1983.

5. Tumojan, E. P. Setevoe obnaruzhenie passivnyh skrytyh kanalov peredachi dannyh v protokole TCP IP / E. P. Tumojan, M. V. Anikeev // Zhurnal «Informacion-noe protivodejstvie ugrozam terrorizma» – 2005. – Vyp. 5.

6. Ronzhin A. F. Rasshirenija informacionnyh protokolov, osnovannyh na otobrazhenijah konechnyh mnozhestv // Diskretnaja matematika. – 2004. – T. 16. – Vyp. 2. – S. 11 – 16.

7. Nazarov, I. V. Razrabotka modeli netradicionnogo informacionnogo kanala i metodov protivodejstvija netradicionnym informacionnym kanalam v setjah paket-noj peredachi dannyh / Nazarov I.V. // Jelektronnyj zhurnal «Trudy Kubanskogo Gosudarstvennogo Agrarnogo Universiteta». - Krasnodar: KubGAU, 2006.

8. Korolev, I. D. Matematicheskaja model' sistemy vyjavlenija skrytyh kanalov / Korolev, I. D., Savchuk D.V., Syzranov A. P., Logvinenko S.V., Myznikov O.N. // Jelektronnyj zhurnal «Trudy Kubanskogo Gosudarstvennogo Agrarnogo Universiteta». - Krasnodar: KubGAU, 2010, № 60 (06).