УДК 621.396.677.49

МЕТОД ПОВЫШЕНИЯ СКРЫТНОСТИ СИГНАЛОВ УПРАВЛЕНИЯ В ПРОГРАММНО-КОНФИГУРИРУЕМОЙ СЕТИ

Ю.Ю. Коляденко, И.Г. Лукинов
Харьковский национальный университет радиоэлектроники

Abstract *– Possible attacks specific to SDN-networks are data corruption, disclosure of information about the network state, denial of service, compromise the switch, interception of traffic, and attack on the control channel. The main attacks on the control channel are considered, which are possible when the switch is compromised. In SDN networks, when communicating sensitive information between the controller and the switch, the problem is to counteract unauthorized access (CUA) or attacks. Unauthorized access to transmitted information involves detecting a signal, determining the structure of a detected signal, and disclosing the information contained in the signal. The listed tasks of the CUA are opposed to three types of stealth signals: energy, structural and information. A method for increasing the stealth of control signals in the SDN network is developed through the use of timed signal structures (TSS). With the help of mathematical modeling, the probability of disclosing the structure of a TSS is determined. As studies showed, the probability of disclosure of the signal structure significantly decreases with the growth of the TSS formation interval. The probability of information concealment of TSS is analyzed depending on the number of analyzed TSS at various parameters. As studies have shown, an increase in the ensemble of realizations and an increase in the number of jointly analyzed constructions reduces the probability of disclosing the semantic content of the transmitted information.*

Анотація *– Розроблено метод підвищення скритності сигналів управління в мережі SDN за рахунок застосування таймерних сигнальних конструкцій (ТСК). За допомогою математичного моделювання визначено ймовірності розкриття структури ТСК. Проведено аналіз ймовірностей інформаційної скритності ТСК в залежності від кількості аналізованих ТСК при різних його параметрах.*

Аннотация *– Разработан метод повышения скрытности сигналов управления в сети SDN за счет применения таймерных сигнальных конструкций (ТСК). С помощью математического моделирования определены вероятности раскрытия структуры ТСК. Проведен анализ вероятностей информационной скрытности ТСК в зависимости от количества анализируемых ТСК при различных его параметрах.*

Введение

Сеть связи характеризуется огромной стоимостью и большими сроками строительства. Изменения в стандартах связи происходят регулярно, но переход к новому стандарту требует новых вложений и замены оборудования, которое часто еще не выработало свой ресурс. Сейчас для запуска сети нового поколения все становится проще благодаря технологии программно-конфигурируемых сетей (SDN). В подобного рода сетях ряд основных функций, связанных с управлением процессами коммутации и маршрутизации, централизованы и вынесены на специальный сетевой контроллер [1, 2].

Взаимодействие между сетевым контроллером и передающими устройствами реализуется посредством программного интерфейса, который используется для прямого управления группами устройств. Наиболее развитым программным интерфейсом на данный момент является протокол OpenFlow [1, 3-7]. Архитектура OpenFlow-коммутатора базируется на одной или нескольких таблицах правил, определяющих механизм обработки потоков сетевого трафика. Каждое правило является записью в

таблице OpenFlow-коммутатора. Запись сопоставляется с определенным потоком трафика. В зависимости от результата сопоставления применяется соответствующее действие (блокирование, передача, модификация и т.д.) к пакетам из данного потока.

Архитектура SDN, предполагая существенно иной подход к реализации сетевой инфраструктуры, не лишена потенциальных уязвимостей с точки зрения информационной безопасности. Необходимость разделения доступа сетевых приложений при работе с контроллером, вопросы аутентификации и авторизации при работе приложений с контроллером – это лишь немногие аспекты безопасности, которые приходится принимать во внимание при проектировании SDN-сетей [1].

Основными компонентами программно-конфигурируемых сетей на базе протокола OpenFlow являются:

1) коммутатор OpenFlow

2) контроллер OpenFlow

3) канал связи, с помощью которого осуществляется взаимодействие контроллера и коммутатора, как правило, для защиты передаваемых сообщений используется TLS, но возможна передача по стандартному TCP без шифрования [4].

Сообщения по каналу связи передаются посредством сигналов, которые атакующий может перехватить и атаковать канал управления, что может повлечь критичные для всей инфраструктуры последствия. Таким образом, разработка метода повышения скрытности сигналов управления в программно-конфигурируемой сети является актуальной научной задачей.

I. Основные атаки и угрозы сети SDN

Возможными атаками, специфичными для SDN-сетей являются [1]:

- искажение данных;
- раскрытие информации о состоянии и статусе сети;
- отказ в обслуживании;
- компрометация коммутатора;
- перехват трафика;
- атака на канал управления.

Рассмотрим основные атаки на канал управления, которые возможны при компрометации коммутатора.

Перехват управляющего трафика.

Атакующий может использовать скомпрометированный коммутатор для перехвата управляющего трафика, через данный коммутатор. Более того, атакующий может перехватить управляющий трафик, посылаемый скомпрометированному коммутатору, если перед этим был произведен перехват управляющего канала. Скомпрометированный коммутатор может быть использован для атак на целостность сети. Атакующий может производить подделку видимого для контроллера состояния коммутатора и создавать поддельные виртуальные коммутаторы в данной сети.

Подделка состояния коммутатора.

Скомпрометированный коммутатор используется атакующим для того, чтобы передавать контроллеру ложные сведения о текущем состоянии данного коммутатора или других коммутаторов, подключенных к контроллеру, через скомпрометированный коммутатор. Например, атакующий может передавать контроллеру ложную информацию о содержимом таблиц потоков, о статистике по трафику или о том, какие интерфейсы имеет коммутатор. Атакующий может подделывать состояния других коммутаторов. Данная атака может быть использована для изменения сетевой топологии. Атакующий может влиять на процесс выбора маршрута для потоков в сети.

Компрометации контроллера.

Приложения, работающие на контроллере, могут содержать в себе уязвимости, эксплуатация которых приведет к компрометации контроллера атакующим. Также приложения могут уже содержать вредоносный код. Большинство современных контроллеров не предоставляют разграничение доступа для приложений на контроллере, что приводит к тому, что каждое приложение может иметь доступ не только к внутренним данным других приложений, но и к внутренним структурам контроллера. Типичной атакой, базирующейся на данных свойствах контроллеров, может быть то, что вредоносное приложение может изменить структуру, содержащую внутреннее представление сети, что приведет к неправильной работе всех приложений на контроллере.

II. Метод повышения скрытности сигналов управления в SDN-сети за счет применения таймерных сигнальных конструкций

В сетях SDN при передаче конфиденциальной информации между контроллером и коммутатором проблемой является обеспечение противодействия средствам несанкционированного доступа (НСД) или атакам [8, 9]. Несанкционированный доступ к передаваемой информации предполагает обнаружение сигнала, определение структуры обнаруженного сигнала и раскрытие содержащейся в сигнале информации. Перечисленным задачам НСД противопоставляются три вида скрытности сигналов: энергетическая, структурная и информационная.

Энергетическая скрытность характеризует способность противостоять мерам, направленным на обнаружение сигнала средствами НСД. Известно [9], что одним из путей повышения энергетической скрытности является увеличение ширины спектра используемых сигналов, что достигается применением шумоподобных (ШПС) и хаотических сигналов в системах конфиденциальной передачи информации.

Структурная скрытность характеризует способность противостоять мерам НСД, направленным на раскрытие структуры сигнала при условии, что сигнал уже обнаружен. Это означает распознавание формы сигнала и измерение его параметров, т.е. отождествление обнаруженного сигнала с одним из множества априорно известных передаваемых символов. Очевидно, что для увеличения структурной скрытности

необходимо иметь по возможности больший ансамбль используемых сигналов с изменяемыми во времени параметрами. Информационная скрытность определяется способностью системы противостоять мерам, направленным на раскрытие смыслового содержания сообщения, передаваемого с помощью сигналов [8]. Раскрытие смыслового содержания означает отождествление каждого принятого сигнала или их множества с тем сообщением, которое передавалось.

Противодействие средствам НСД является важнейшей задачей, поэтому следует осуществлять поиск и исследование методов передачи, позволяющих увеличить скрытность сигналов управления в сетях SDN. В данной работе рассматривается возможность повышения скрытности сигналов бинарного канала за счет применения таймерных сигнальных конструкций (ТСК) [10].

Известно, что индивидуальные двоичные каналы имеют базу $B = 1$ и используют избыточный код. Эффективность [9] использования двоичного канала можно повысить за счет таймерного метода формирования сигнальных конструкций на заданном интервале n – элементного избыточного кода. Сигнальный алфавит бинарных таймерных сигнальных конструкций для каждого индивидуального канала формируется на интервале времени $T_c = nt_0$ (t_0 – величина, обратная полосе пропускания канала ΔF) при базовом элементе Δ ($\Delta = \frac{t_0}{S}$, $S = 1,2,...,k$ – целые числа).

Пример формирования сигнального алфавита бинарных ТСК на интервале времени $T_c = 7t_0$ при базовом элементе Δ показан на рис. 1.

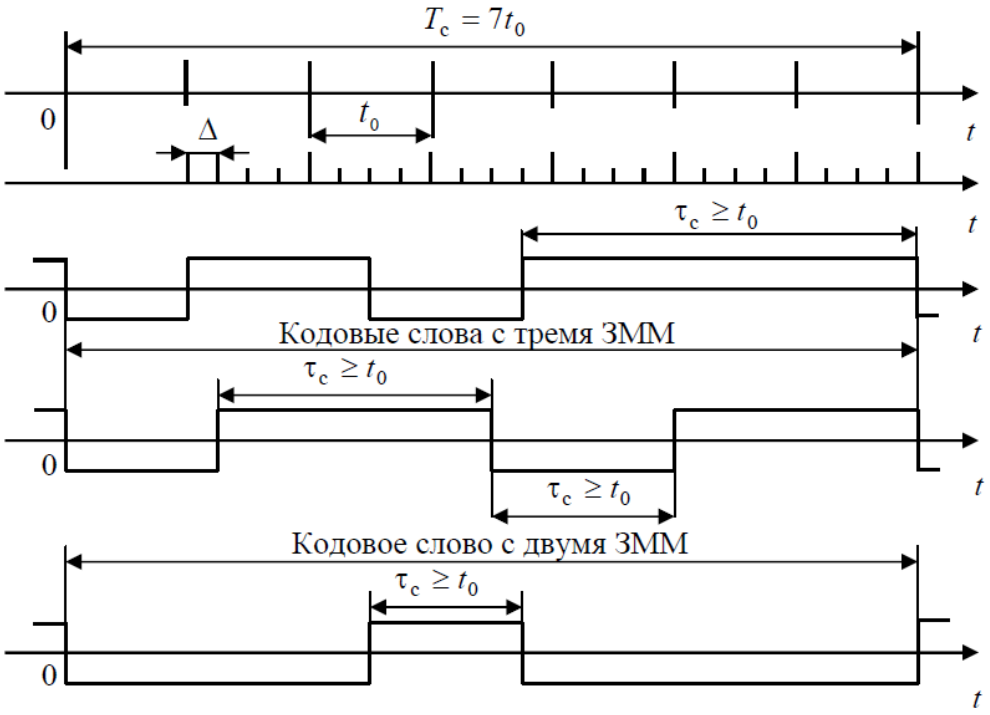

Рис. 1. Формирование сигнального алфавита бинарных ТСК на интервале времени $T_c = 7t_0$ при базовом элементе Δ

Каждый значащий момент модуляции (ЗММ) может занимать на интервале формирования ТСК позиции, расположенные на расстоянии $k\Delta \geq t_0$ друг от друга по отношению к предыдущему, причем Δ определяется как минимальное расстояние между соседними положениями одного ЗММ в разных конструкциях. Информация о передаваемом сообщении, переносимая ТСК, содержится в номере временной позиции, занимаемой ЗММ.

Из рисунка видно, что в каждой сигнальной конструкции сигнал с длительностями Δ в канал не передается. Однако длительность элемента Δ учитывается, когда на приеме производится оценка поступившей конструкции в сравнении со всеми возможными реализациям.

III. Метод повышения скрытности сигналов управления в сети SDN за счет применения таймерных сигнальных конструкций

Определению информационной скрытности предшествует оценка структурной скрытности сигналов. Рассмотрим возможность увеличения ансамбля передаваемых сигналов при использовании ТСК. Известно [10], что множество реализаций бинарных ТСК формируется на интервале времени $T_c = nt_0$, где n – количество элементарных посылок, а t_0 – их длительность.

Базовым элементом при формировании является ТСК $\Delta = \frac{t_0}{S}$. В отличие от разрядно-цифрового кода (РЦК), когда информация о передаваемом разряде определяется уровнем сигнала элементарной посылки, в ТСК информация заложена в нескольких отдельных (временных) интервалах сигнала $\tau_c = t_0 + k\Delta$, где $k = 0,1,2,..S(n-2)$ и их на интервале T_c взаимном положении. С одной стороны такой метод формирования дает возможность передавать в канал отрезки сигнала длительностью $\tau_c \geq \Delta \cdot (S+i)$, где $i = 0,1,2,3...$ (i – число информационных ЗММ в сигнале), что исключает межсимвольные искажения в каналах с базой $B = 1$. С другой стороны не кратность τ_c величине t_0 позволяет уменьшить расстояния между сигнальными конструкциями до величины $\Delta < t_0$ и получить число реализаций ТСК N_{TCKp} на интервале nt_0 значительно больше $2n$ [10]:

$$N_{TCKp} = \sum_{i=1}^{n} \frac{[(n \cdot S) - [(S-1)i]]!}{i![[(n \cdot S) - [(S-1)i]] - i]!}. \quad (1)$$

Число реализаций ТСК с учетом значений S, n и $i = 1,...,n$ приведено в табл. 1. Анализ таблицы показывает, что кодек ТСК позволяет сформировать значительно больше разрешенных ТСК на одном и том же интервале, чем кодовых слов РЦК, где число реализаций $N = 2^n$. Например, при формировании ТСК на интервале $T_c = 5t_0$ и $S = 7$ число возможных реализаций $N_{TCKp} = 1293$. Такое количество реализаций можно получить только с помощью простого двоичного кодового слова с длиной $n = \log_2 1293 = 11$ элементов.

Таблица 1. Количество реализаций ТСК при различных значениях S и n

n \ S	1	2	3	4	7	10	15	20
5	31	88	188	344	1293	3310	10475	24940
8	255	1596	5895	16492	153400	735450	4952841	20628612
10	1023	10945	58424	217224	3705000	27042520	302000000	1830000000

На рис. 2 показана упрощенная структурная схема системы передачи конфиденциальной информации с использованием ТСК. Источник информации выдает непрерывную последовательность информационных двоичных элементов РЦК, которая кодеком ТСК разбивается на блоки некоторой длины РЦК k.

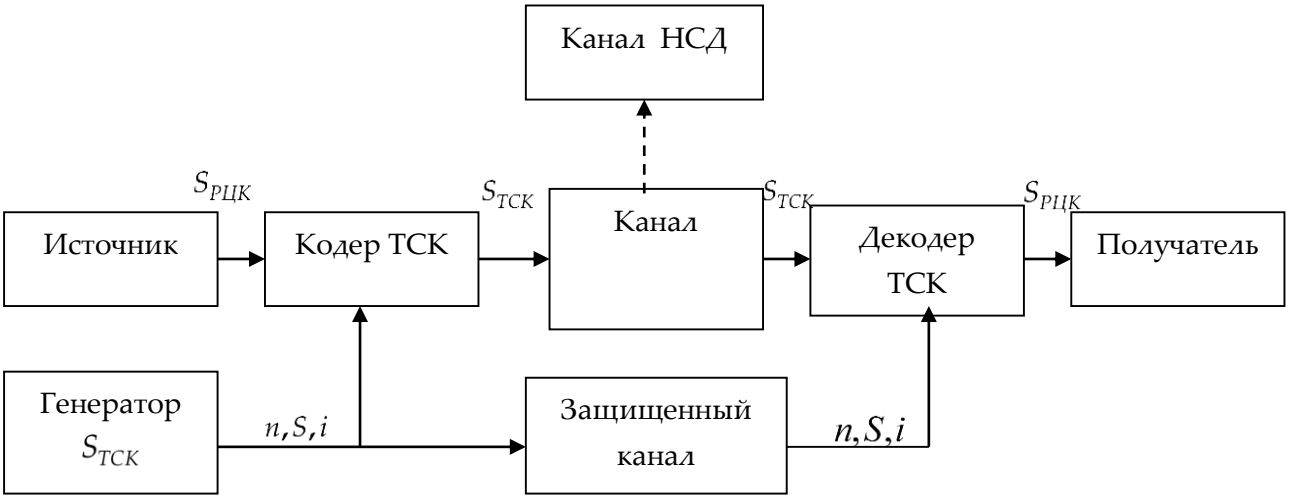

Рис. 2. Структурная схема системы передачи конфиденциальной информации

Длина блока РЦК k определяется из условия максимально возможного числа реализаций N_{TCKp}, сформированных на некотором интервале n при выбранных параметрах S и i, тогда:

$$k_{РЦК} \le \mathbf{log}_2 N_{TCKp}. \quad (2)$$

Каждой длине блока РЦК k соответствует число, определяющее номер реализации РЦК. Кодер ТСК осуществляет кодирование сигнала РЦК $S_{РЦК}$ в сигнал ТСК S_{TCK} по правилу:

$$S_{РЦКj} \to S_{TCKz} \quad (n,S,i), \quad (3)$$

т.е. каждый сигнал $S_{РЦКj}$ представляется определенной конструкцией S_{TCKz}, где j и z – соответственно номера реализаций.

Изменение параметров n,S,i дает возможность на выходе кодера ТСК получать различные множества сигнальных конструкций, каждое из которых может отличаться длительностями, зависящими от значений n, числом базовых элементов S и числом переходов i, т. е. структурой сигнала. Например, при определенных значениях n и S можно формировать различные множества конструкций S_{TCKz} изменением только числа переходов i, где каждому его значению будет соответствовать множество со своей структурой сигнала. Аналогично, изменением S и n или различных допустимых комбинаций n,S,i можно на выходе кодера ТСК получать множества S_{TCKz} с разной формой сигнала. Частота смены параметров кодером ТСК выбирается такой, чтобы объем перехваченных станцией НСД реализаций ТСК определенной формы с заданными параметрами был не достаточен для раскрытия структуры сигнала в пределах интервалов времени, представляющих практический интерес. Так как параметры n,S,i должны быть известны приемной стороне, то их передача обычно осуществляется по отдельному достаточно защищенному каналу.

Наличие априорной и апостериорной неопределенностей делает задачу определения структуры сигнала вероятностной, поэтому количественной мерой структурной скрытности таймерной сигнальной конструкции может служить вероятность раскрытия структуры сигнала $p_{стр}$ при условии, что сигнал уже обнаружен. Следовательно, $p_{стр}$ представляет собой условную вероятность, и ее определение заключается в нахождении параметров n,S,i.

Для получения максимально возможной структурной скрытности, т. е. достижения минимальной $p_{стр}$, последовательность символов сообщения в кодере должна подлежать такому преобразованию, при котором различные символы в его выходной последовательности появлялись бы по возможности равновероятно. Следовательно, при передаче, например, текста, использующего алфавит из 32 букв, каждая из которых появляется с разной вероятностью, необходимо кодировать не отдельные буквы, а последовательности из различных (учитывающих и порядок) сочетаний букв, чем можно обеспечить достаточно равновероятное появление сигналов на выходе кодера. Но увеличение алфавита приводит к возрастанию ансамбля реализаций, что требует дополнительных затрат, например, увеличения длительности передачи или расширения ширины спектра канала связи, что не всегда желательно. Например, при кодировании последовательностей из двух букв первичный ансамбль реализаций $N = 32$ увеличивается и принимает значение $N = 32^2 = 1024$, что приводит к необходимости использования для передачи такого ансамбля 10-элементного РЦК вместо 5-элементного.

Применение кодера ТСК дает возможность на интервале 5-элементного РЦК при параметрах n=5, S=7 и $i = 1\ldots n$ (табл. 1) сформировать достаточный ансамбль реализаций:

$$N_{TCKp} = 1293 > N_p = 1024,$$

чтобы оставить длительность передачи без изменений.

Значение $p_{стр}$ определяется с учетом минимального ансамбля реализаций A_{TCK}, который требуется проанализировать методом полного перебора для нахождения ключей n, S и i при несанкционированном доступе:

$$p_{стр} = \frac{1}{A_{TCK}}, \tag{4}$$

где

$$A_{TCK} = \sum_{n} \sum_{S} \sum_{i=1}^{n} \frac{[(n \cdot S) - [(S-1)i]]!}{i!\,[[(n \cdot S) - [(S-1)i]] - i]!}. \tag{5}$$

С помощью математического моделирования определены вероятности раскрытия структуры ТСК в зависимости от значений n, S и i. На рис. 3 приведены графики вероятностей раскрытия структуры ТСК в зависимости от значений n при S =1 (верхняя кривая), S=6 (средняя кривая) и S=12 и i =1 … n. Как видно из рисунка, вероятности раскрытия структуры сигнала $p_{стр}$ существенно уменьшаются с ростом интервала T_c формирования ТСК.

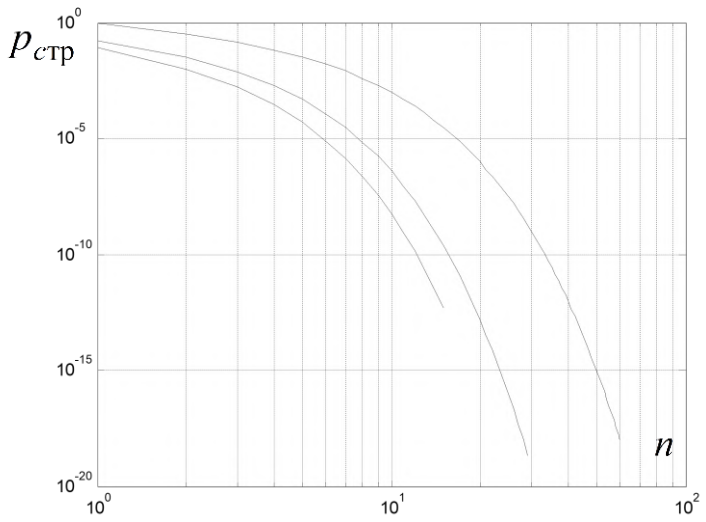

Рис. 3. График вероятностей раскрытия структуры ТСК в зависимости от значений n при S =1, S=6, S=12 и i =1 … n

Раскрыв структуру сигнала, станция НСД располагает набором параметров n, S и i для определения его информационной скрытности.

Предположим, что система передачи использует простой двоичный код, тогда смысловое содержание может быть раскрыто путем анализа соответствий реализаций ТСК реализациям РЦК. Количество сравнений для одной реализации с учетом известных n, S и i определяется выражением:

$$N_{РЦК} = N_{TCK} = \frac{[(n \cdot S) - [(S-1)i]]!}{i![[(n \cdot S) - [(S-1)i]] - i]!}, \quad (6)$$

где N_{TCK} и $N_{РЦК}$ – соответственно число реализаций ТСК и РЦК.

Однако для определения смыслового содержания информации необходимо анализировать не одну ТСК, а совместно некоторое их количество в N_{TCK}. В этом случае необходимое число сравнений $A_{инф}$ будет определяться выражением:

$$A_{инф} = C_{N_{TCK}}^{N_{aTCK}}. \quad (7)$$

Задача определения информационной скрытности сигнала также является статистической, поэтому в качестве количественной меры информационной скрытности можно принять условную вероятность раскрытия смыслового содержания передаваемой информации $p_{инф}$, заложенной в обнаруженном сигнале с раскрытой структурой. Учитывая, что таймерные конструкции на выходе кодера ТСК равновероятны, а их таблицы перекодировки в РЦК меняются по определенному (известному на приемной стороне) алгоритму, значение определяется формулой:

$$p_{инф} = \frac{1}{A_{инф}}. \quad (8)$$

Например, на приемной стороне для каждого числа переходов i в принятой реализации ТСК при определенных значениях n и S используется своя таблица перекодировки в РЦК. Также разным S или некоторым комбинациям параметров n, S и i могут соответствовать другие таблицы, что повышает информационную скрытность передаваемых сигналов. Частота смены параметров n, S, i и соответствующих им таблиц перекодировки выбирается такой, чтобы накопленные станцией НСД статистические данные по числу перехваченных реализаций ТСК не давали возможности достаточно быстро распознать смысловое содержание передаваемого сообщения.

На рис. 4 приведены графики вероятностей информационной скрытности ТСК в зависимости от количества анализируемых ТСК при различных значениях n, S и i. Как видно из рисунка, увеличение ансамбля реализаций N_{TCK} и рост числа совместно анализируемых конструкций N_{aTCK} уменьшает вероятность $p_{инф}$.

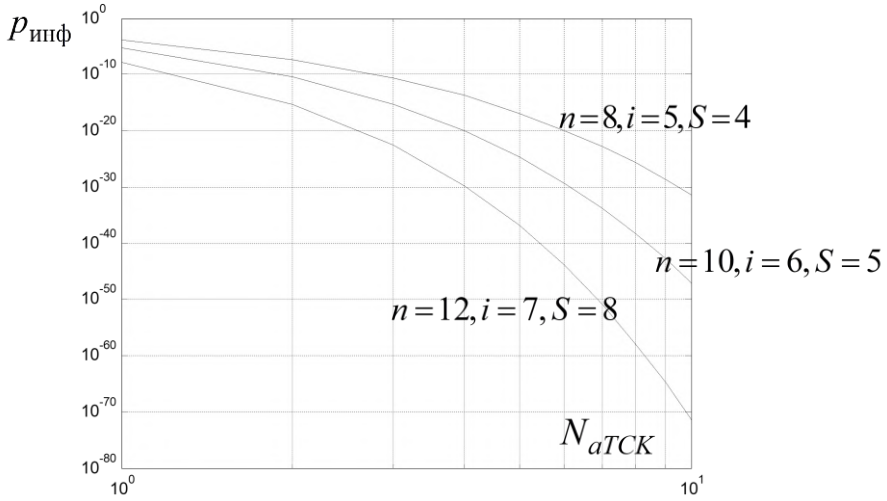

Рис. 4. Графики вероятностей информационной скрытности ТСК в зависимости от N_{aTCK} при различных значениях n, S и i

Выводы

1. Возможными атаками, специфичными для SDN-сетей являются: искажение данных; раскрытие информации о состоянии и статусе сети; отказ в обслуживании; компрометация коммутатора; перехват трафика; атака на канал управления. Рассмотрены основные атаки на канал управления, которые возможны при компрометации коммутатора.

2. В сетях SDN при передаче конфиденциальной информации между контроллером и коммутатором проблемой является обеспечение противодействия средствам несанкционированного доступа или атакам. Несанкционированный доступ к передаваемой информации предполагает обнаружение сигнала, определение структуры обнаруженного сигнала и раскрытие содержащейся в сигнале информации. Перечисленным задачам НСД противопоставляются три вида скрытности сигналов: энергетическая, структурная и информационная. Разработан метод повышения скрытности сигналов управления в сети SDN за счет применения таймерных сигнальных конструкций.

3. С помощью математического моделирования определены вероятности раскрытия структуры ТСК. Как показали исследования вероятности раскрытия структуры сигнала $p_{стр}$ существенно уменьшаются с ростом интервала T_c формирования ТСК. Проведен анализ вероятностей информационной скрытности ТСК в зависимости от количества анализируемых ТСК при различных его параметрах. Как показали

исследования, увеличение ансамбля реализаций и рост числа совместно анализируемых конструкций уменьшает вероятность раскрытия смыслового содержания передаваемой информации.

Список литературы:

1. *Захаров А. А., Попов Е.Ф., Фучко М. М.* Аспекты информационной безопасности архитектуры SDN // Вестник СибГУТИ. – 2016. № 1. – С. 83 – 92.

2. *McKeown N., Anderson T., Balakrishnan H., Parulkar G., Peterson L., Rexford J., Shenker S., Turner J.* Openflow: enabling innovation in campus networks // ACM SIGCOMM Computer Communication Review. – 2008. – 38 (2). – P. 69–74.

3. OpenFlow Switch Specification Ver 1.5.1, 2016 [accessed January 11, 2016]. https://www.opennetworking.org/images/stories/downloads/sdnresources/onf-specifications/openflow/openflow-switch-v1.5.1.pdf.

4. *Партыка Т.Л., Попов И.И.* Информационная безопасность / Учебное пособие для студентов учреждений среднего профессионального образования. — М.: ФОРУМ: ИНФРА-М, 2002. − 368с.

5. OpenFlow Switch Specification, Version 1.1.0 Implemented. – Режим доступу: www.openflow.org/documents/openflow-spec-v1.1.0.pdf

6. OpenFlow white paper. – Режим доступу: www.archive.openflow.org/documents/openflow-wp-latest.pdf.

7. *McKeown N., Anderson T., Balakrishnan H., Parulkar G., Peterson L., Rexford J., Shenker S., Turner J.* OpenFlow: Enabling Innovation in Campus Networks // SIGCOMM Comput. Commun. – Rev. March. – 2008. – Vol. 38. – P. 69–74.

8. *Куприянов А.И., Сахаров А. В.* Теоретические основы радиоэлектронной борьбы. – М.: Вузовская книга, 2007. – 356 с.

9. *Борисов В. И., Зинчук В. М., Лимарев А. Е. и др*. Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью / под ред. В. И. Борисова. – М.: Радио и связь, 2003. – 640 с.

10. *Захарченко Н. В., Крысько А. С., Захарченко В. Н.* Основы кодирования: учебное пособие. – Одесса: УГАС им. А. С. Попова, 1999. – 240 с.