УДК 621.396.677.49

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ АТАК И ЗАЩИТ В ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЯХ

Ю.Ю. Коляденко
Харьковский национальный университет радиоэлектроники
А.П. Глушко
Харьковский национальный университет Воздушных Сил имени Ивана Кожедуба
А.И. Воронин
Национальная академия Национальной гвардии Украины

Abstract *– Distinctive features of the construction of wireless urban telecommunication networks are the high complexity of the medium access control protocol, which is responsible, in particular, for providing subscribers with access to a common communication channel, as well as the presence of a large number of uncertain parts in which only some of the network interaction mechanisms are standardized. These features of the SDN technology, as well as its novelty, lead to the need to develop methods for improving information security in the case of multiple radio access by subscribers. The task of ensuring security is becoming especially relevant for telecommunication networks, where the data transmission channel is often shared between a large number of users. In wireless metropolitan area networks, another problem appears - the general availability of the communication channel. The article discusses the active way of organizing the fight against unauthorized interference with the Software-Defined Network (SDN). Proactive measures are planned based on known vulnerability data of software products. An open NVD database is used. The forecast of the most dangerous threats is carried out in the form of a game between two partners: the attacker and the defender. The result of the game is recommendations for the protection of information for the investigated software system. The analysis is carried out to determine the equilibrium states and stability of the dynamic system. For this purpose, a phase portrait is built, i.e. the dependence of the state of threats on the effectiveness of attacks is obtained. As the analysis has shown, with greater attack efficiencies, a smaller sampling interval is needed to maintain the system in an equilibrium state.*

Анотація *– У статті розглядається активний спосіб організації боротьби з несанкціонованим втручанням у роботу мережі зв'язку SDN. Попереджувальні заходи плануються на базі відомих даних про уразливість програмних продуктів. Використовується відкрита база даних NVD. Прогноз найбільш небезпечних загроз проводиться у формі гри двох партнерів: того, хто атакує, та того, хто захищається. Підсумок гри - рекомендації щодо захисту інформації для досліджуваної програмної системи. Проведено аналіз для визначення рівноважних станів і стійкості динамічної системи. Для цього побудовано фазовий портрет, тобто побудована залежність стану загроз від ефективності атак. Як показав аналіз, при більшій ефективності атак необхідний менший інтервал дискретизації для підтримки системи в рівноважному стані.*

Аннотация *– В статье рассматривается активный способ организации борьбы с несанкционированным вмешательством в работу программно-конфигурируемой сети связи SDN. Упреждающие мероприятия планируются на базе известных данных об уязвимости программных продуктов. Используется открытая база данных NVD. Прогноз наиболее опасных угроз проводится в форме игры двух партнеров: атакующего и защищающегося. Результат игры – рекомендации по защите информации для исследуемой программной системы. Проведен анализ для определения равновесных состояний и устойчивости динамической системы. Для этого построен фазовый портрет, т.е. построена зависимость состояния угроз от эффективности атак. Как показал анализ, при больших эффективностях атак необходим меньший интервал дискретизации для поддержания системы в равновесном состоянии.*

Введение

В настоящее время значительный интерес представляют исследования беспроводных городских телекоммуникационных сетей, в которых имеется центральная станция, координирующая работу абонентских станций. Именно такая архитектура является основой технологии программно-конфигурируемых сетей (Software-

Defined Networks, SDN). Отличительными особенностями построения беспроводных городских телекоммуникационных сетей являются высокая сложность протокола подуровня управления доступом к среде, отвечающего, в частности, за организацию доступа абонентов к общему каналу связи, а также наличие большого числа неопределенных частей, в которых стандартизированы лишь некоторые механизмы сетевого взаимодействия. Эти особенности технологии SDN [1-7], а также ее новизна, приводят к необходимости разработки методов повышения защиты информации при множественном радиодоступе абонентов.

Задача обеспечения безопасности становится особенно актуальной для телекоммуникационных сетей, где канал передачи данных часто разделяется между большим количеством пользователей. В беспроводных городских сетях появляется еще одна проблема — общедоступность канала связи [8]. Поэтому для обеспечения безопасности беспроводных городских сетей необходимо проведение детального анализа возможности возникновения несанкционированного доступа при тех или иных вариантах развития ситуации. В этих целях разрабатываются математические модели. Таким образом, проведение анализа существующих моделей и методов обеспечения информационной безопасности, а также разработка модели взаимодействия атак и защит является актуальной научной задачей.

Объектом исследования является процесс организации безопасности в беспроводных программно-конфигурируемых сетях связи SDN.

Предмет исследования составляют модели взаимодействия атак и защит.

Целью данной работы является разработка модели взаимодействия атак и защит, а также проведение анализа и предоставление рекомендаций по обеспечению информационной безопасности.

I. Постановка задачи

Рассматривается активный способ организации борьбы с несанкционированным вмешательством в работу сети связи SDN. Упреждающие мероприятия планируются на базе известных данных об уязвимости программных продуктов. Используется открытая база данных NVD. Прогноз наиболее опасных угроз проводится в форме игры двух партнеров: атакующего и защищающегося. Результат игры – рекомендации по защите информации для исследуемой программной системы [1].

Способы защиты информации от несанкционированного или ошибочного вмешательства носят обычно пассивный характер. Такова защита с помощью пароля (частного и общего), шифрация, создание туннеля безопасности, использование шлюзов – барьеров и т. п. Идеология пассивной, не изменяемой защиты не может быть эффективной в течение длительного времени [6, 7]. Виды атак на аутентификацию, текст и ресурс постоянно меняются и становятся все более изощренными. Поэтому необходимо совершенствовать подход и методы, применяемые для защиты [1-3]. Изначально пассивность защиты основывается на недооценке уже существующих угроз. Не принимаются во внимание высокие темпы изменения услуг связи, быст-

рый прогресс программно-алгоритмического обеспечения, запаздывание развития связного оборудования. Все это создает благоприятные условия для опережающего нападения в пределах уже известной уязвимости объекта атаки.

Упреждающий подход к формированию защиты информации основан на том, что в настоящее время накоплен и систематизирован экспериментальный материал, позволяющий оператору защиты с высокой достоверностью предполагать, как будет организована атака на информацию как на объект нападения. Можно выдвинуть гипотезу, какие атаки следует парировать в первую очередь. Для повышения степени достоверности прогноза атак и защит необходимо построение теоретико-игровой модели, реализующей антагонистическую стратегию.

II. Модель динамики взаимодействия и фазовые состояния атак и защит

Анализ взаимодействия атак и защит можно представить в виде теоретико-игровой модели [9-11]. Игра – это математическая модель коллективного поведения: несколько участников влияют на ситуацию, причем их интересы (выигрыши или потери при различных возможных ситуациях) различны. При таком представлении во взаимодействии динамических систем S_i, $i=\overline{1,n}$ возможны три характерные стратегии поведения. В общем случае эти стратегии могут быть классифицированы следующим образом:

1) антагонистическая стратегия, когда участники имеют противоположные интересы;

2) кооперативная стратегия, когда у всех игроков есть общая цель и их стратегии согласованы;

3) стратегия равнодушия или игра с природой, когда стратегия j-го игрока не зависит от стратегии i-го игрока.

Известны и другие типы стратегий – чистые или смешанные [9]. Игра в чистых стратегиях предполагает детерминистский подход, и как следует из теории, редко приводит к равновесным решениям. В противоположность этому для игр в смешанных стратегиях при стохастическом подходе круг равновесных решений значительно расширяется.

Очевидно, что процессы атак и защит представляются антагонистической стратегией или в общем виде – смешанной. При небольших отклонениях в информации об априорных данных поведение такой системы можно представить моделью взаимодействий и фазовых состояний атак и защит. Следует отметить, что в известных работах отсутствует представление телекоммуникационной сети в виде теоретико-игровой модели с антагонистической стратегией поведения.

Основные параметры и состояния атак $x_i(t)$ обычно известны, и часто их можно принять детерминированными. Случайным является макросостояние всей группировки сети SDN [9, 11]. Данное обстоятельство объясняется влиянием множества не-

определенных, случайных условий. В результате случайных угроз от атак $y_i(t)$, $i=\overline{1,n}$, где n – число атак, состояния параметров атак изменяются. В сети имеются соответствующие динамические взаимодействия, которые могут быть выявлены и проанализированы в результате измерений и наблюдений, и характеризуются вектором $\vec{y}(t)$. Динамику случайных изменений состояния параметров атак можно описать системой дифференциальных уравнений:

$$\frac{d\vec{x}(t)}{dt} = F(t)\vec{x}(t) + B(t)\vec{u}(t) + G(t)\vec{\xi}(t), \quad (1)$$

где $\vec{x}(t)$ – вектор состояния параметров атак, $F(t)$ и $B(t)$ – матрица состояния и управления соответственно, $\vec{u}(t)$ – вектор управления соответствующими параметрами, $\vec{\xi}(t)$ – порождающий процесс, часто аппроксимирующийся белым гауссовым шумом, отображающий случайный механизм, $G(t)$ – матрица, масштабирующая случайные возмущения $\vec{\xi}(t)$.

Наблюдаемые параметры состояния угроз атак описываются системой алгебраических уравнений:

$$\vec{y}(t) = R(\vec{x}(t), t), \quad (2)$$

где $R(\cdot)$ – матрица наблюдения.

При этом можно предположить, что если весь вектор атак наблюдаем, то предпринимаются меры по их предотвращению, т.е. производится защита с той или иной вероятностью.

В общем случае система уравнений (1) может быть нелинейной. Тогда без конкретизации самой нелинейности векторное уравнение (1) может быть представлено в виде:

$$\frac{d\vec{x}(t)}{dt} = F\Phi[\vec{x}(t), \vec{y}(t)], \quad (3)$$

где F – матрица состояния размерности $n \times n$, при этом $F = \mathrm{diag}(f_i, i \in \overline{1,n})$, если x_i независимы.

Успешность решения задачи защит по отношению к атакам зависит от наличных ресурсов $g_k = g_k(\vec{x}(t), t)$, $k \in \overline{1,K}$, а также от известных априорных вероятностей $p_i = p_i(\vec{x}(t), t); i \in \overline{1,n}$.

При наличии динамики изменения состояния системы во времени, уравнение (3) можно представить в виде:

$$\frac{d\vec{x}(t)}{dt} = K\Phi[\vec{x}(t), \vec{y}(\vec{x}(t), t)]. \quad (4)$$

Наличные ресурсы g_k определяются физическими величинами. Весь ресурс можно представить в виде взвешенной суммы наблюдаемых величин:

$$g_k(\vec{x}(t),t)=\sum_{i=1}^{n}c_{ik}y_i,\ y_i\ge 0,\ k\in\overline{1,K},\ i\in\overline{1,n}\ , \tag{5}$$

где c_{ik} – наличие связи между i-й атакой и k-й защитой. Соответствующие связи определяются матрицей C, которая состоит из нулей и единиц, определяющих наличие или отсутствие таких связей.

В сети, как и в любой динамической системе, в процессе функционирования осуществляется перераспределение ресурсов, определяемое моделями стационарных состояний, которые описываются задачами максимизации энтропии [11]:

$$H(Y)=\mathbf{max}\left[\sum_{i=1}^{n}y_i\ \mathbf{ln}\frac{p_i}{y_i}+y_i\right] \tag{6}$$

при соответствующих ограничениях на ресурсы.

Динамика состояния процесса определяется решением $\vec{y}(t)$ задачи (3), которое, как следует из (5) и (6), зависит от ее параметров p_i, c_{ik} и g_k. Таким образом, модель динамики состояния атак приобретает следующий вид:

$$\frac{d\vec{x}(t)}{dt}=\Phi[\vec{x}(t),\vec{y}(\vec{x}(t),t)], \tag{7}$$

$$\vec{y}(\vec{x}(t),t)=\mathbf{arg\,max}\left[H(Y)\left|\sum_{i=1}^{n}c_{ik}y_i=g_k(\vec{x}(t),t)\right.\right]. \tag{8}$$

В рассматриваемой неравновесной системе имеют место два основных процесса (потока): атак и угроз от атак. Обозначим через $\Phi[\vec{x}(t),\vec{y}(t)]$ – поток атак, а $Q[\vec{x}(t),\vec{y}(t)]$ – поток угроз от атак. Эти потоки зависят от состояния $\vec{x}(t)$ и состояния $\vec{y}(t)$. В рамках предположений о том, что время угрозы атаки больше времени появления самой атаки [9-11], можно записать следующую, в общем случае нелинейную систему уравнений:

$$\frac{d\vec{x}(t)}{dt}=\Phi[\vec{x}(t),\vec{y}(\vec{x}(t),t)], \tag{9}$$

$$\varepsilon\frac{d\vec{y}(t)}{dt}=Q[\vec{x}(t),\vec{y}(\vec{x}(t),t)], \tag{10}$$

где ε – диагональная матрица, определяющая эффективность атак в сети.

Формирование модели вида (10) для процесса с ограничениями и разнотипными ресурсами пока остается нерешенной задачей [11]. Такую модель удается построить лишь для тех случаев, когда динамика процесса – марковская, для ограничений балансового типа. В рассматриваемом случае можно предположить, что динамика процесса является марковской, поскольку не имеет значения, когда и как сеть перешла в текущее состояние, а существенно лишь то, в каком состоянии сеть находится в данный момент времени.

Рассматривается достаточно общий случай наличия n атак в сети SDN. Вектор защит является функцией численности атак $\vec{z} = f(y_1, ..., y_n)$. При отсутствии атак $(y_1 = ... = y_n = 0)$ имеем $\vec{z} = f(0)$. В обратном случае при очень большом их количестве $(y_1 \to \infty, ..., y_n \to \infty)$ – $\vec{z} = f(\infty) \to 0$. Наличие достаточно большого числа атак ведет к сбоям, т.е. к увеличению вероятности возникновения неравновесных состояний. Скорость изменения i-й атаки определяется появлением новых атак $k_i y_i$, (веса k_i можно принять постоянными $k_i = const$) и исчезновением старых $g_i y_i$ при условии воздействия защиты. Коэффициенты g_i зависят от количества ресурса u_i, затрачиваемого в среднем на одну атаку, $g_i = g_{i0} - \mu_i u_i$; $g_{i0}, \mu_i > 0$, (μ_i – вес управляющего воздействия на i-ю атаку). Тогда

$$\frac{dy_i(t)}{dt} = \varepsilon_i y_i(t) + \mu_i w_i(t), \qquad i \in \overline{1, n}, \tag{11}$$

где $w_i = u_i(t) y_i$ – количество ресурса, затрачиваемого на i-ю атаку; $\varepsilon_i = k_i - g_i$.

Будем рассматривать стационарные состояния процесса при фиксированных на момент времени t взаимодействиях атак и защит.

Для этого процесса можно указать некоторую априорную характеристику. Для каждой i-й атаки обычно известно нормативное количество ресурса a_i, и следовательно параметр ν_i:

$$\nu_i = \frac{a_i y_i}{\sum_{i=1}^{n} a_i y_i}; \quad 0 \le \nu_i \le 1; \quad \sum_{i=1}^{n} \nu_i = 1. \tag{12}$$

Стационарное состояние такого процесса определяется моделью вида [5]

$$H(w) = \sum_{i=1}^{n} (w_i \ln \frac{\nu_i}{w_i} + w_i) \to \max. \tag{13}$$

С учетом (12), получим:

$$w_i^* = a_i y_i \frac{\sum_{i=1}^{n} w_i}{\sum_{i=1}^{n} a_i y_i}.$$

После подстановки этого выражения в (11) получаем:

$$\frac{dy_i}{dt} = y_i(\varepsilon_i + a_i \varphi(y)), \tag{14}$$

где $\varphi(y) = \frac{\sum_{i=1}^{n} w_i}{\sum_{i=1}^{n} a_i y_i}$, которые будут монотонно убывать для $y_i \ge 0$.

В этом случае коэффициенты ее линейной аппроксимации отрицательны, т.е.

$$\varphi(Y) = \sum_{s=1}^{n} \nu_s y_s(t). \quad (15)$$

Подставив (15) в (14), получим систему Вольтерра, характеризующую динамику сосуществования атак и защит в условиях антагонистической игры [9]:

$$\frac{dy_i(t)}{dt} = y_i(t)(\varepsilon_i - \sum_{s=1}^{n} \nu_s y_s(t)). \quad (16)$$

Если использовать для описания функции $\varphi(y)$ квадратичную аппроксимацию, то получим нелинейную систему Вольтерра, описывающую состояния взаимодействия атак и защит, т.е. состояние угроз от атак:

$$\frac{dy_i(t)}{dt} = y_i(t)(\varepsilon_i - \sum_{s=1}^{n} \nu_s y_s(t) - \sum_{s=1}^{n}\sum_{j=1}^{n} \nu_s y_s(t) v_j y_j(t)). \quad (17)$$

Преобразуем данное дифференциальное выражение к разностному. Обозначим через t_k дискретное время, тогда

$$\frac{dy_i(t_{k+1}) - dy_i(t_k)}{t_{k+1} - t_k} = y_i(t_k)(\varepsilon_i - \sum_{s=1}^{n} \nu_s y_s(t_k) - \sum_{s=1}^{n}\sum_{j=1}^{n} \nu_s y_s(t_k) v_j y_j(t_k)),$$

где $t_{k+1} - t_k = T_d$ – интервал дискретизации.

Тогда для дискретного времени получим разностное уравнение

$$y_i(k+1) = y_i(k) + T_d[y_i(k)(\varepsilon_i - \sum_{s=1}^{n} \nu_s y_s(k) - \sum_{s=1}^{n}\sum_{j=1}^{n} \nu_s y_s(k) v_j y_j(k))]$$

или

$$y_i(k+1) = y_i(k) \cdot (1 + T_d)(\varepsilon_i - \sum_{s=1}^{n} \nu_s y_s(k) - \sum_{s=1}^{n}\sum_{j=1}^{n} \nu_s y_s(k) v_j y_j(k)). \quad (18)$$

Данная модель позволяет выполнять анализ при различных конкретных параметрах и взаимодействий атак и защит.

III. Анализ модели динамики взаимодействия и фазовые состояния атак и защит

Рассмотрим динамику неравновесных состояний (18) угроз от атак при различных значениях ε, учитывающих эффективность атак.

Вначале проведем исследование состояний угроз от атак при интервале дискретизации $T_d = 1$. Физический смысл данного параметра в том, что мониторинг состояния сети и акт защиты производится столько раз, сколько производится атак.

С помощью имитационного моделирования проведен анализ динамики взаимодействий и фазовых состояний атак и защит сети SDN при различных эффектив-

ностях атак. На рис. 1 представлена зависимость угроз от атак $y_1(t)$ и $y_2(t)$ при малой эффективности атак $\varepsilon << 1$. Номера кривых соответствуют номеру атаки. На рис. 2 представлена зависимость угроз от атак $y_1(t)$ и $y_2(t)$ при малой эффективности атак $\varepsilon \approx 1$.

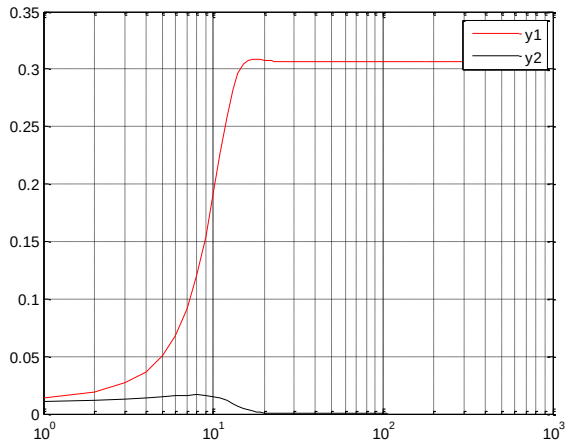

Рис. 1. Зависимость угроз $y_1(t)$ и $y_2(t)$ при малой эффективности атак $\varepsilon << 1$; $\varepsilon_1 = 0,4; \quad \varepsilon_2 = 0,1$

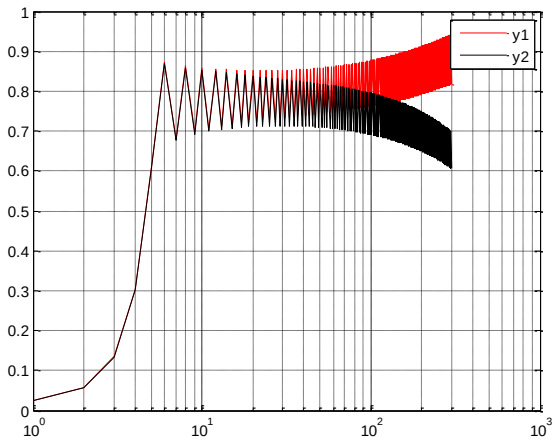

Рис. 2. Зависимость угроз $y_1(t)$ и $y_2(t)$ при средней эффективности атак $\varepsilon \approx 1$; $\varepsilon_1 = 1,41; \quad \varepsilon_2 = 1,409$

Как видно из рис. 1, при малых, но различных значениях ε, угрозы от атак возрастают до наступления установившегося режима. Различие состоит в том, что $\varepsilon_1 > \varepsilon_2$. Физический смысл данного неравенства состоит в том, что первая атака создает большую угрозу по сравнению со второй атакой. Поэтому и влияния $y_1 > y_2$.

При значениях $\varepsilon \approx 1$ (рис. 2) отмечаются две характерные области графиков. Начальная область, где отмечается резкое увеличение угрозы, как от первой, так и второй атаки и стационарная, неравновесная часть с последующими заметными колебаниями во времени, что связано с перераспределением угроз и защит.

Проанализирован случай работы сети при больших значениях интенсивностей $\varepsilon >> 1$ (рис. 3), при которых система приобретает запредельное насыщенное состояние. Полученные результаты, представленные на рис. 3, свидетельствуют о том, что при достаточно больших значениях эффективности атак динамика состояния сети становится непредсказуемой: может происходить как резкое увеличение угроз, так и резкое снижение, характерное для тех ситуаций, которые возникают в сети при нештатном режиме работы, появляется так называемый детерминированный хаос.

Проведем анализ для определения равновесных состояний и устойчивости динамической системы. Для этого построен фазовый портрет, т.е. построена зависимость состояния угроз y от параметра ε. На рис. 4. представлен фазовый портрет динамической системы при $T_d = 1$. Судя по фазовому портрету (рис. 4), критическим числом ε при $T_d = 1$, при котором сеть еще не теряет устойчивости, является $\varepsilon \cong 1,4$.

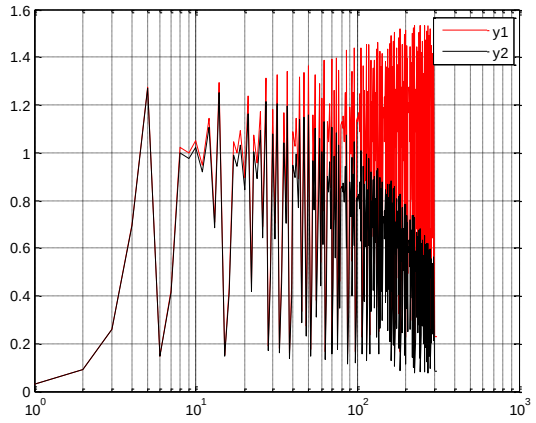

Рис. 3. Зависимость угроз $y_1(t)$ и $y_2(t)$ при $\varepsilon \approx 1;\ \varepsilon_1 = 2,01;\quad \varepsilon_2 = 2,008$

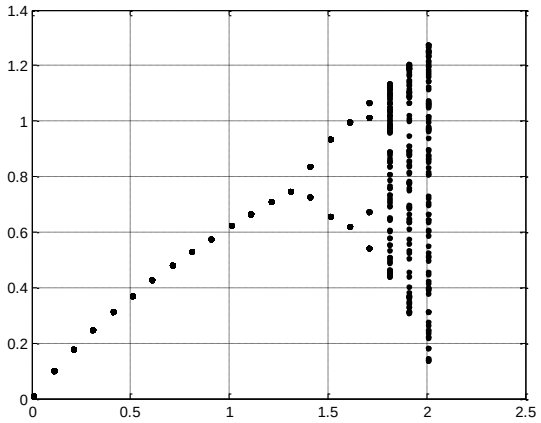

Рис. 4. Фазовый портрет динамической системы при $T_d = 1$

Из данного графика следует, что в области $\varepsilon > 1,4$ наступают раздвоения траекторий (бифуркация состояния). В области $\varepsilon \geq 1,4$ изменения состояния наблюдаемой системы могут оказаться значительными и неоднозначными при незначительных изменениях эффективности атак. Проведены исследования состояний угроз от атак при интервале дискретизации $T_d = 0,1$. То есть мониторинг состояния сети и акт защиты производится в 10 раз чаще поступления атак.

На рис. 5 представлены графики зависимости угроз от атак $y_1(t)$ и $y_2(t)$ при малой эффективности атак $\varepsilon << 1$. Номера кривых соответствуют номеру атаки. На рис. 6 представлены графики зависимости угроз от атак $y_1(t)$ и $y_2(t)$ при средней эффективности атак $\varepsilon \approx 1$. Проанализирован случай работы сети при больших значениях интенсивностей $\varepsilon >> 1$ (рис. 7), при которых система приобретает запредельное насыщенное состояние $\varepsilon_1 = 13;\quad \varepsilon_2 = 12,97$.

Как видно из рис. 5, при малых, но различных значениях ε, угрозы от атак возрастают до наступления установившегося режима. Различие состоит в том, что $\varepsilon_1 > \varepsilon_2$. При этом, сравнивая графики рис. 1 и рис. 5, можно сделать вывод о том, что угроза от атаки происходит намного медленнее (на порядок) при $T_d = 0,1$, чем при $T_d = 1$. При значениях $\varepsilon \approx 1$ (рис. 6) отмечается 2 области графиков. Начальная область, где отмечается переходной режим, как первой, так и второй атаки, и нестационарная, неравновесная часть. Кроме того, переходной режим происходит гораздо быстрее, чем при $\varepsilon << 1$ (рис. 5). При больших значениях интенсивностей (рис. 7) состояние сети становится непредсказуемым при значениях эффективностей атак на много больше, чем при $T_d = 1$.

Проведен анализ для определения равновесных состояний и устойчивости динамической системы. Для этого построен фазовый портрет, т.е. построена зависимость состояния угроз y от параметра ε. На рис. 8. представлен фазовый портрет динамической системы при $T_d = 0,1$.

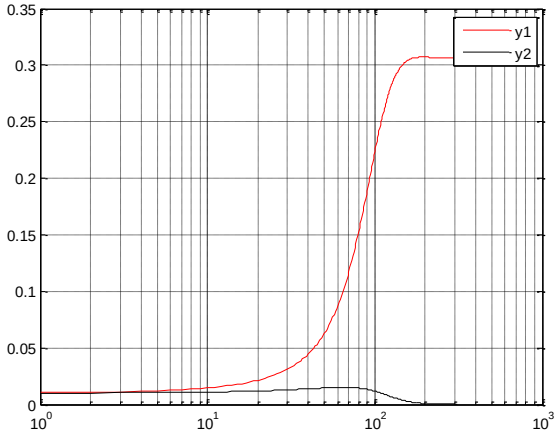

Рис. 5. Зависимость угроз $y_1(t)$ и $y_2(t)$ при малой эффективности атак $\varepsilon << 1$; $\varepsilon_1 = 0,4;\quad \varepsilon_2 = 0,1$

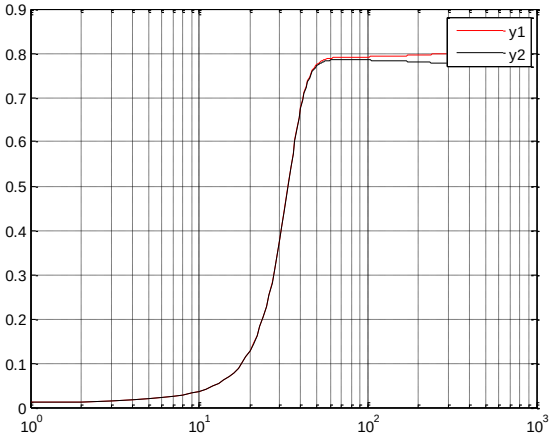

Рис. 6. Зависимость угроз $y_1(t)$ и $y_2(t)$ при средней эффективности атак $\varepsilon \approx 1$; $\varepsilon_1 = 1,41;\quad \varepsilon_2 = 1,409$

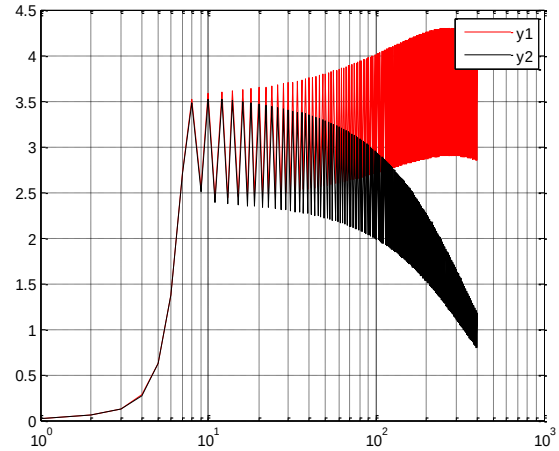

Рис. 7. Зависимость угроз $y_1(t)$ и $y_2(t)$ при больших значениях эффективности атак $\varepsilon >> 1$; $\varepsilon_1 = 13;\quad \varepsilon_2 = 12,97$

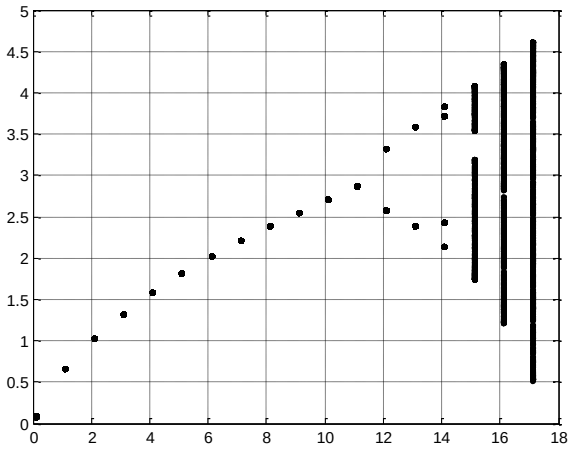

Рис. 8. Фазовый портрет динамической системы при $T_d = 0,1$

Судя по фазовому портрету, при $T_d = 0,1$ (рис. 8) неравновесное состояние наступает при эффективности угроз $\varepsilon = 11$, что по сравнению с предыдущим примером при $T_d = 1$ почти на порядок больше. Как показал анализ, при больших эффективностях атак необходим меньший интервал дискретизации для поддержания системы в равновесном состоянии.

Выводы

В работе нашла дальнейшее развитие теоретико-игровая модель, где реализована антагонистическая стратегия. На основании создания базы данных уязвимости программного обеспечения удается поставить задачу прогнозирования наиболее

эффективных угроз информационной безопасности конкретного объекта атаки. Задача прогноза может быть поставлена как игра двух лиц: атакующего и защищающегося. Адекватность такой постановки задачи следует из возможности рассмотрения плоскости платежной матрицы игры как поля состояний объекта в процессе изменения его состояний.

Получены результаты анализа неравновесных состояний в группировке сети, позволяющие доказать возможность наличия равновесных состояний и определить границы устойчивости функционирования динамических взаимодействующих сетей при различных значениях эффективности угроз и различных интервалах дискретизации. Анализ показал, что при большой эффективности атак необходим меньший интервал дискретизации для поддержания системы в равновесном состоянии.

Список литературы:

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

2. *Коляденко Ю.Ю., Лукинов И.Г.* Модель выявления и устранения уязвимостей в программно-конфигурируемых сетях связи на основе аппарата марковских процессов // Радиотехника Всеукр. межвед. научн.-техн. сб. — 2017. — Вып. 189. — С. 148-154.

3. *Kolyadenko Yu.Yu., Lukinov I.G.* A model for disclosure and elimination of vulnerabilities in the software-defined communication networks based on the markovian processes // Telecommunications and Radio Engineering. – 2018. — № 77(4). – P. 327-336. DOI: 10.1615/TelecomRadEng.v77.i4.40

4. *Коляденко Ю.Ю., Білоусова К.Е.* OpenFlow-based software-defined networking // Technology audit and production reserves. — 2016. — № 2 (28). — С. 9-13.

5. *Коляденко Ю.Ю., Білоусова К.Е.* Организация программно-конфигурируемой сети на базе протокола OpenFlow // Технологический аудит и резервы производства. — 2016. — № 2(2). — С. 9-13.

6. *Коляденко Ю.Ю., Білоусова К.Е.* Программно-конфигурируемые сети на базе протокола OpenFlow и их характеристики // ScienceRise. — 2016. — № 2 (20). — С. 11-16.

7. *Коляденко Ю.Ю., Лукинов И.Г.* Модель распределенных атак в программно-конфигурируемых сетях связи // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2017. – Т. 17, № 3. – С. 34–43.

8. *Лукацкий А.* Информационная безопасность 2015 // ИТ-безопасность. Стандарты. Средства защиты. Мероприятия. — 2013. — № 12. — С.64-69.

9. *Коляденко Ю.Ю.* Анализ взаимодействия и фазовые состояния группировки радиоэлектронных средств систем абонентского радиодоступа // Прикладная радиоэлектроника. — 2004. — Т. 3, №3. — С. 37-42.

10. *Коляденко Ю.Ю., Величко Т.В.* Модель динамики неравновесных состояний при распределении ресурсов в сети абонентского радиодоступа // Радиотехника. — 2005. — Вып. 142. — С. 34-39.

11. *Лесик Р.А.* Теоретико-игровая модель атак в городских беспроводных сетях // Материалы XVII Международного молодежного форума «Радиоэлектроника и молодежь в XXI веке». — Харьков, 2013. — С. 103-104.